UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

PRIVACY POLICY DYNAMICS IN LOCATION SHARING APPLICATIONS

Luís Fernandes Sousa

Mestrado em Segurança Informática

Novembro 2009

UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

PRIVACY POLICY DYNAMICS IN LOCATION SHARING APPLICATIONS

Luís Fernandes Sousa

Tese orientada pelo Prof. Doutor Norman M. Sadeh
e co-orientada pelo Prof. Doutor Nuno Ferreira Neves

Mestrado em Segurança Informática

Novembro 2009

Resumo

As aplicações de partilha de localização (*location-sharing*) prometem modificar, de uma forma radical e num futuro bastante próximo, a forma como as pessoas interagem e socializam, estabelecendo a ponte entre as redes sociais e o mundo real. No entanto, as preocupações, legítimas e generalizadas, relativas às implicações de privacidade associadas a esta classe de aplicações, sugerem que a sua adopção por parte da comunidade dependerá sempre da medida em que essas preocupações sejam resolvidas. Uma dificuldade adicional consiste no facto de os utilizadores deste tipo de aplicações têm dificuldade em antecipar a forma de utilizar o serviço, e em definir filtros (políticas de privacidade) que traduzam essas mesmas preocupações.

Vários grupos de investigação têm analisado as necessidades e comportamentos desses utilizadores, com o objectivo de identificar um conjunto de mecanismos que resolva efectivamente essas necessidades. Até à data, ainda não existem publicações que explorem a dimensão temporal nas análises efectuadas. Assim sendo, este projecto visa compreender o comportamento ao longo do tempo de utilizadores do Locaccino, uma aplicação de partilha de localização desenvolvida e concretizada pelo *Mobile Commerce Lab*. Mais especificamente, o projecto visa identificar elementos-chave que não são revelados sem ter em consideração a dimensão temporal e a ordenação dos eventos, aproveitando o facto de o Locaccino permitir estudos de longa duração.

Foram analisados os comportamentos e preferências de privacidade de 289 utilizadores do Locaccino, divididos por 2 estudos. Os resultados revelam que os utilizadores, ao modificar as suas preferências de privacidade (filtros), evoluem tipicamente para políticas menos restritivas, partilhando mais localizações. Os mesmos utilizadores evoluem simultaneamente para preferências de privacidade tipicamente mais complexas, o que sugere a existência de um processo de aprendizagem (mensurável) ao longo do tempo. Foi ainda analisada de mecanismos que de transparência (feedback) que permitem aos utilizadores saber informação sobre quem tenta obter as suas localizações. Os resultados revelam a importância dos mecanismos de transparência (*feedback*) para ajudar os utilizadores na construção das suas políticas de privacidade. Esta importância é mais visível nos utilizadores com terminais móveis.

A integração destes resultados no desenvolvimento de aplicações de partilha de localização resultará seguramente numa maior eficácia das políticas de privacidade definidas pelos utilizadores, aumentando assim o seu conforto relativamente às questões de privacidade.

Palavras-chave: privacidade, análise dinâmica, partilha de localização, plataformas móveis.

Abstract

Location-sharing applications in social networking may radically transform the way people interact and socialize with each other, by providing the bridge between social networking and the actual social interaction. People already expressed legitimate concerns about the privacy implications associated with this class of applications, suggesting that a broad adoption may only happen to the extent that these concerns are adequately addressed. Additionally, users still cannot anticipate how the location-sharing service is going to be used, or how to express the privacy policies that most suite their needs.

A significant research effort has already been put in the analysis of user's needs, for building user-controllable systems that adequately protect the disclosure of their locations. However, no published work has yet explored the temporal dimension in such analyses. This project aims at studying people's attitudes and behaviors towards privacy using Locaccino, a location-sharing application developed and deployed by the Mobile Commerce Lab. More specifically, it aims at identifying key elements that are only revealed with a dynamic analysis of usage data that takes into consideration the temporal dimension and the ordering of events, based on the fact that Locaccino allows long-last studies.

We analyzed the privacy preferences and behavior of 289 Locaccino users, in two distinct studies. Our results demonstrate that users, when modifying their policies, typically evolve to less restrictive, sharing more locations. They also evolve to more complex privacy policies, suggesting an increasing awareness of the implications of their decisions over time. We investigated the importance of mechanisms that provide users with awareness of who tried to locate them (feedback mechanisms). The results reveal the importance of feedback mechanisms for helping users defining their privacy policies, which is particularly relevant for those using mobile platforms.

We believe that the integration of these findings in the design of location-sharing applications can significantly contribute to enhance the effectiveness of user's privacy policies.

Keywords: privacy policy, dynamic analysis, location sharing technology, mobility.

Acknowledgements

This thesis symbolizes a professional and personal dream that could not be made true without the invaluable support of my family, colleagues, universities and sponsor.

I would like to thank Carnegie Mellon University, Faculty of Sciences at the University of Lisbon (Faculdade de Ciências da Universidade de Lisboa), CMU|Portugal and Portugal Telecom for their support during the last 16 months.

To Professor Norman Sadeh and Eran Toch for their guidance and suggestions.

To my MSIT-IS colleagues for their companionship throughout this program.

To my family, who suffered the most with my full-time dedication to this project.

Dedicated to my soul mate, Rita.

Table of Contents

1 Introduction 1

1.1. Location technology 1

1.2. Privacy and security concerns 2

1.3. Privacy policies and user behavior 2

1.4. Organization of the document 3

2 Background 5

2.1. Theories 5

2.1.1. Privacy theories 5

2.1.2. Role-based access control models 6

2.1.3. Design principles for secure systems 6

2.2. Related work 7

2.2.1. Privacy and location-sharing 7

2.2.2. Policy analysis 9

3 Research method 11

3.1. Model 11

3.1.1. Definitions 11

3.1.2. Privacy policies and location requests' evaluation 11

3.1.3. Privacy policy management taxonomy 12

3.1.4. Restrictiveness 13

3.1.5. Openness 14

3.1.6. Dynamic analysis of privacy policies 15

3.1.7. Feedback hypothesis 16

3.2. Framework 18

3.2.1. Methodology 18

3.2.2. Dynamic analysis 18

3.3. Locaccino 19

3.3.1. Web application 20

3.3.2. Locators 23

3.4. Experiment 26

3.4.1. Long-term users study 26

3.4.2. Mobile study 27
4 Results 31
4.1. Long-term users study results 31
4.1.1. Experiment design parameters 31
4.1.2. Static analysis 32
4.1.3. Dynamic analysis 35
4.2. Mobile study results 39
4.2.1. Static analysis 39
4.2.2. Dynamic analysis 42
5 Discussion 47
5.1. Implications for design 47
5.2. Future work 48
5.3. Location-sharing evolution 48
6 Conclusions 51
7 References 53

List of Figures

Figure 1 – Example of dynamic analysis of privacy policies 15
Figure 2 - Feedback condition illustration 17
Figure 3 - Methods for capturing user's feedback 18
Figure 4 – Locaccino home page 21
Figure 5 – Locaccino privacy settings page 22
Figure 6 - Locaccino "Who can locate me" page 23
Figure 7 - Locaccino "Who's located me" (feedback) page 24
Figure 8 – Laptop locator (Windows OS) 25
Figure 9 – Mobile locator 25
Figure 10 – Locaccino user's experience duration 27
Figure 11 – Time duration of Locaccino user's activity 32
Figure 12 – Group-based restrictiveness distribution 34
Figure 13 – Time-based restrictiveness distribution 34
Figure 14 – Dynamics of long-term aggregate (all users) location requests 35
Figure 15 - Dynamics of privacy policy expressiveness (per iteration) 36
Figure 16 – Use of expressiveness according to privacy policy restrictiveness trend 37
Figure 17 – Aggregated cumulative restrictiveness dynamics 38
Figure 18 – Privacy policy expressiveness distribution for laptop and smartphone users 41
Figure 19 – Dynamics of laptop user's location requests 42
Figure 20 - Dynamics of smartphone user's location requests 43
Figure 21 – Dynamics of mobile study user's aggregate (normalized) restrictiveness 43
Figure 22 – Dynamics of laptop user's aggregate (normalized) restrictiveness 44
Figure 23 - Dynamics of smartphone user's aggregate (normalized) restrictiveness 44

List of Tables

Table 1 – Location mechanism's characterization 1
Table 2 – Activity time period for long-term users 27
Table 3 – Privacy policy management parameters' characterization 32
Table 4 – Long-term user's characterization in terms of location requests and openness 33
Table 5 – Expressiveness (static) characterization of long-term users 34
Table 6 – Comparison between feedback and no-feedback groups (long-term users) 39
Table 7 – Location requests and respective evaluation for laptop and smartphone users 40
Table 8 – Laptop versus smartphone user's comparative openness 40
Table 9 – Privacy policy management temporal characterization 41

“Liberty exists in proportion to wholesome restraint;

The more restraint on others to keep off from us, the more liberty we have.”

Daniel Webster

1 Introduction

1.1. Location technology

The most commonly used location mechanisms are Wi-Fi positioning, cellular identification and Global Positioning System (GPS). Any of these mechanisms have enough accuracy for the location-sharing requirements.

Wi-Fi localization mechanism consists in assigning users with the location of Wi-Fi access points. While Wi-Fi public access points provide limited coverage, the increasing adoption of personal wireless devices has severely increased the global coverage in urban areas (even indoors). Researchers and companies such as Skyhook Wireless [1] have created large databases with considerable granularity, to be used with this location mechanism.

Cellular identification is based on measuring power levels and antenna patterns. It relies on the assumption that a mobile phone always communicates wirelessly with one of the closest base stations. The accuracy of this technology depends on the concentration of base stations, ranging from 50 meters in urban areas up to miles in rural areas. Some companies interested in the location-sharing market are partnering with telecom companies in order to use cellular data with location purposes.

GPS locates a person through a device (held by the person) that is in communication with a constellation of satellites. Its accuracy reaches the magnitude of few meters, depending of factors like the receiving antenna and the morphology of the terrain. Despite being the most accurate location mechanism, it requires line-of-sight (outdoor environments) and can be battery intensive.

The applicability of these location mechanisms depend mostly on the coverage, accuracy and power consumption.

Location mechanism	Accuracy	Coverage	Indoors	Battery consumption
Wi-Fi	High (DB dependent)	Urban areas	Yes	Regular
Cellular	Low (BTS dependent)	Mobile telephony's	Yes	Low
GPS	Highest	Worldwide	No	Intensive

Table 1 – Location mechanism's characterization

While laptops are currently equipped with Wi-Fi, smartphones are increasingly being equipped with all the three location mechanisms, which tend to be considered a "must have" feature [2]. Whenever more than one location mechanism is available in a given device, the one preferred is usually the one that ensures enough coverage, maximizes the accuracy while minimizing the power consumption. In section 3.3.2, we describe the specific location technologies implemented in our location-sharing application, Locaccino.

1.2. Privacy and security concerns

The ubiquity of location information raises both benefits and privacy concerns for location-based applications [3], since locations become more invaluable. Security concerns also arise if perpetrators are able to gain access to location information about their victims, e.g., increasing the risk of stalking and domestic violence.

Compared to general location-aware applications, location-sharing applications have an added value in selectively sharing one's location. For example, in a location-aware social network this can be a social benefit like meeting a nearby friend. A distinct example of application is parental control, where the disclosure of a child's location allows attesting the child's safety. In fact, parental control is an application where the need for selective disclosure is evident for ensuring both privacy and security.

People's concerns with location privacy may depend on the place, not only in terms of their physical location but also in terms of their social context: their personal definition of where they are, what they are doing, and with whom [4]. Moreover, people that tend to be more concerned about privacy in general are the ones that most vary their willingness to share location information.

A recent study [5] revealed that most Internet users have concerns about sharing their location information online, are extremely concerned about controlling who has access to their locations and feel the risks of using location-sharing technologies outweigh the benefits. They also feel that the most likely harms would stem from revealing the location of their home to others or being stalked.

One additional concern is the fact that location information is highly identifiable, even when anonymized [6]. Most people have one location where they spend their daytime hours (workplace) and one location where they spend their nighttime (home). One week of collecting just two data points about a person may fairly reveal the identity of the person.

Location data may also indirectly describe what a person is doing through contextual inference. For example, frequent visits to clinics signal medical problems, attending meetings may reveal political preferences, and meetings with influential business managers could indicate pending business deals. As such, the problem of sharing location information is analogous to hospitals publishing medical records to epidemiologists and other medical researchers – it can beneficial to society but invades on privacy.

1.3. Privacy policies and user behavior

Privacy concerns raised by location-sharing were rapidly perceived by potential users, suggesting that a broad adoption may only happen to the extent that these concerns are adequately addressed. Despite their concern with their privacy, users cannot

anticipate how the location-sharing service is going to be used or the privacy policies that most suite their privacy concerns.

Therefore, it is crucial to fully understand the user's behavior when using location-sharing applications in order to address their privacy concerns with an adequate design of user interfaces. This will most likely raise users' comfort with location sharing and also severely reduce the probability of rejection.

In this project we analyze the user's behavior through time, specifically in terms of their privacy policies expressiveness (the type of restrictions being used and the way they are combined) and restrictiveness (how open/restrictive these policies are).

1.4. Organization of the document

The rest of this document is organized as follow. In chapter 2 we present the theories that supported the design and evolution of our location-sharing application, Locaccino. In chapter 3 we present the formal model and research methodology required for this type of project. This chapter also includes a description of Locaccino. In chapter 4 we present our results based on two studies, the first one intended to provide general insights, and the second one more focused in the specific aspects of users with mobile devices. Chapters 5 and 6 contain the discussion and the conclusions of this project.

2 Background

Theories of both privacy and computer systems design are relevant for the study of privacy in location-sharing applications. We present some of these theories and also related work on the same topic.

2.1. Theories

We first present a brief description of the evolution of privacy theories. Then, we present role-base access control (RBAC), a predominant model for advanced security and privacy, which is used in the design of privacy policies (rules) in our location-sharing application (Locaccino). Finally, we list some of the design principles for secure systems and refer to how they are implemented in the same application.

2.1.1. Privacy theories

The demand for full protection in person and in property is a principle as old as the common law. The exact nature and extent of such protection, as well as the challenge of dealing with the intangibility, were the main concerns that led to the definition of the right to privacy, still in the IXX century by Warren and Brandeis [7]. At that time, the right "to be let alone" was written largely in response to the increase in newspapers and photographs that invaded the sacred precincts of private and domestic life. The impact of the right to privacy was later emphasized by Justice Williams O. Douglas, as being the abutment of all freedom, in the sense that people have as much freedom as the restraint on others to keep off from them.

More recently, Altman's privacy regulation theory [8] presented privacy as a dynamic process that can change through time and is conditioned by both internal and external conditions. Altman also differentiates privacy desired levels from the actual levels of privacy achieved, defines an optimal level of privacy for each individual that not necessary the highest, and defines a two level hierarchy for privacy (individual and group privacy).

This project makes use of Altman's notion of privacy as a dynamic process of interpersonal boundary, by investigating the boundary interactions that condition how open or how closed is the individual's attitude in regard to his/her location disclosure at any given moment.

There has been significant discussion on the concept of information privacy as more and more systems controlling more information appear. Nevertheless, the existing global data privacy framework (APEC) has been recurrently criticized as incoherent and inefficient.

2.1.2. Role-based access control models

Role-based access control (RBAC) is a widely accepted access control reference model as it significantly simplifies the paradigm of permission management. The permissions to perform certain operations are assigned to specific roles, therefore, users acquire permissions through their role and not through directly assignment. Permission management is significantly simplified with RBAC.

In one of the first known works [9], the RBAC main concepts were presented, as well as the formal description of role and membership. In [10], a family of RBAC models is introduced and the role is presented as being the intermediary that brings together a collection of users, on one side, and a collection of permissions, on the other.

Role-based access control models are applied for access control in Locaccino, namely with respect to the disclosure of locations of users. Its application is straightforward, making the intermediation of the Facebook groups and the privacy policies (rules). Locaccino makes use of Facebook social network, thus, the social groups are not pre-defined. Instead, when users define their Facebook groups they are defining the groups that are used for access control – the group-based restrictions.

Locaccino time-based and location-based restrictions are not relevant for roles. These forms of access control can be seen as a form of context-based access control (CBAC), but where the context is relative to the entity that provides the permissions.

2.1.3. Design principles for secure systems

Saltzer and Schroeder [11] had presented a set of design principles in 1974 that became universally accepted by the computer science and security community. Locaccino system design follows these principles, namely in the way privacy policies (rules) are implemented.

Mechanism economy

This principle states that the design of a system must be as simple and small as possible. Note however that privacy policies are inherently complex. Therefore, the types of restrictions and functionalities implemented in Locaccino user interface are the ones considered the less possible to adequately address user's privacy concerns.

Fail-safe defaults

This principle states that all defaults must be fail-safe, i.e., conservative by default. In Locaccino, this is done by using default rules with maximum restrictiveness. When a user joins Locaccino, his or her location cannot be disclosed unless there is a rule modification. In other words, the default rule is "Deny All Requests".

Complete mediation

This principle states that every access to every object must be checked for authorization. The fact that all location requests are evaluated by the rule set (privacy policy) defined by the target user (authority) ensures the complete mediation.

Psychological acceptability

This principle refers to the usability, one of the main drivers of all the Locaccino design, namely in the user interface. For example, the usability in Locaccino user interface is ensured by the economy of the information displayed to the users (avoiding the user burden), by providing comprehensive functionalities to users, etc.

Avoiding conflicts

Despite not being referred in [11], avoiding conflicts is an important principle in the generic context of filtering and access control, which is why it is referred in [9].

The simplest way of avoiding conflicts is by using exclusively one of the two mechanisms of filtering: whitelist or blacklist. Locaccino implements whitelist mechanisms solely (e.g., allow the location to a give user at a given daytime), therefore avoiding conflicts with economy of mechanisms. Alternatively, one could use whitelist and blacklist but relying in additional layers to detect, prevent and solve eventual conflicts.

2.2. Related work

Recent developments in geographical positioning and location-managing technologies combined with the generalized ubiquity of locatable devices (laptops, mobile phones) sustained the recent multitude of platforms in the market for location-sharing applications. Current examples of commercial location-sharing applications are Google Latitude, Yahoo Fire Eagle, Xtify, Loopt and Four Square[12][13][14][15][16].

A recent study [5], based on an online survey of American Internet users, revealed that most users are extremely concerned about controlling who has access to their locations. The same study revealed that, in general, the privacy controls in existing applications do not comprehensively address user's privacy concerns.

Next we present related work in several areas of privacy and location-sharing, and policy analysis.

2.2.1. Privacy and location-sharing

From a high-level perspective, past work on location privacy can be grouped into three distinct categories: computational, architectural and human aspects (user interface) [17]. The first two categories are intended to protect anonymity of a set of users, to limit what location information is collected and how that information can be queried.

Our project focuses on the third category: the human aspects and user interfaces. Projects in this category are usually divided in the following specific areas of research: usability, expressiveness, and (more recently) mobility.

Usability

Since location sharing rules are inherently complex and users typically cannot picture ahead of time all of their privacy concerns, the user interface must somehow provide some help along the process.

In [17], the usefulness of a wide variety of functionalities is evaluated. One such example is the obfuscation of the evaluation of a location request, where the requestor cannot distinguish if the request is denied by a rule or simply because the target user is offline. Another example is a last seen functionality, which is considered uncomfortable privacy-wise for increasing the risk of tracing.

The importance of feedback (the user being provided with information of who tried to locate him/her) is addressed in [18]. The study reveals the importance of this functionality for increasing the comfort of users with respect to sharing locations. The conclusion is achieved based on the comparison of the levels of privacy concerns of two groups of users: one that was provided with the feedback functionality and the other, from which the functionality remained hidden in the application. Feedback is important not only for awareness but also for deterrence, in the sense that users become more selective when requesting other's locations if they are aware of the existence of feedback mechanisms in the application.

Machine learning was used for deriving adequate default policies for helping users converge faster to their final privacy policies in [19]. The default rules are referred to be necessarily canonical and in small number (e.g., three rules), and some default rules are derived.

Expressiveness

The question of how much expressiveness and exactly which type of filters are required for user interfaces is central to location-sharing applications. Early work in [17][20] has identified the concerns of users to be mapped in the interfaces. The authors identified as being relevant, not only the type of rules to be implemented in the interfaces but also the granularity of the information disclosed. Interestingly, there does not seem to be consensus between the two analyses on whether obfuscation techniques are important in the location-sharing context.

In [18], the specific types of rules that users considered as being useful were group-based, time-based, location-based and proximity rules. The first three are already implemented in Locaccino, and were used in our study. In [20], the proximity of home address had already been identified by users as important to be implemented in user interfaces.

An area of intensive research is location labeling (or naming). The fact that location labels ("home", "workplace", etc) are more meaningful to users than, e.g., their coordinates, makes location naming particularly important for the acceptability of location based rules. One interesting finding in [21] is that people are more open to sharing their location information in the form of place names than exact positions.

An interesting element related to privacy policy expressiveness is granularity, generally considered by users as being useful [19]. However, granularity is not necessarily desired by users for disclosing less location information. In [20], one of the conclusions is that some users just want to provide less information so that the information is more meaningful to the requestor. This type of granularity may also be associated to the distance between requestor and the target in this interaction.

Mobility

Early work on modeling the mobility of people using computers and mobile phones was presented in [22]. Here mobility is classified into three distinct classes: nomadic, cellular and pervasive.

Today's combination of pervasive computing and location-sharing brings enhanced mobility and opportunities to share locations and in more diverse contexts compared to the prior laptop scenario, but it also changes the location-sharing privacy and usability paradigm. Privacy concerns becomes even higher for smartphone users, and the constraints related to the smartphones (intermittent connectivity, reduced display dimensions, battery issues) result in additional challenges in terms of usability.

In [23], an analysis of the smartphone security model for location-sharing is provided. The authors conclude that in this model, users may be interested in defining their group-based privacy policies not only based on the social network (e.g., Facebook) but also based on the contacts (which are typically distinct). Like in prior work, the proximity is referred by users as an important criterion for deciding whether to disclose or not the location.

In [24], the uniqueness of locations visited by mobile users is presented as a factor that raises the privacy concerns related to the disclosure of those specific locations. This is a surprising result, in the sense that it demonstrates that mobile users are more comfortable sharing a location like their home rather than other locations visited occasionally. This may reveal a higher concern with privacy compared to security. An additional conclusion of this study is that mobile users generate more activity (location requests), visit more unique locations and have higher privacy concerns than laptop users.

2.2.2. Policy analysis

Understanding what level of control users need for protecting their privacy in location-sharing applications may be achieved through the analysis of user's privacy policies (rules).

An example of policy analysis approach in the context of file sharing is presented in [25], based in data mining techniques. The context of file sharing has similarities with location-sharing, in the sense that rules are inherent complex. However, unlike in location sharing, users typically do not change their access control settings through

time. An interesting conclusion is that the complexity of rules can be decomposed in simpler (canonical) rules.

3 Research method

In this chapter we start by presenting the model that formally describes users' privacy policies and location requests. We follow by describing our framework aimed at understanding the dynamics of location-sharing user's behavior when using a location-sharing application: Locaccino. We then describe Locaccino with some detail.

Lastly, we describe the two experiments that compose this project, highlighting the recruitment methodology and providing a generic characterization of the populations under analysis.

3.1. Model

In this section we present the necessary formalism to be used in the subsequent analysis of both privacy policies and location requests. We adapted the formal model defined in [26] for the current implementation of Locaccino privacy policies and the specific scope of this project, as follow.

3.1.1. Definitions

A **privacy policy** is a set of condition/action pairings that specify what actions should be taken under what circumstances. It is composed by a set of rules connected by logical disjunction. A **rule** describes the restrictions under which a given set of **actions** (disclose, withhold) may be executed. These **restrictions** are defined as a logical conjunction of their elementary components (e.g., group-based, time-based, location-based restrictions).

We consider a small set of **events** from the universe of all Locaccino system events: the location requests. Events (location requests) necessarily imply the evaluation of a privacy policy, resulting in a given action (disclose, withhold).

A user is in a given **condition** if at least one of his/her policy modifications verifies the corresponding hypothesis.

3.1.2. Privacy policies and location requests' evaluation

The following formal model describes the privacy policies and the evaluation of location requests given the target user's privacy policy.

Rule = ℙ(Restriction x Action)

Policy = ℙ(Rule)

Evaluate:: Policy x Event $\rightarrow$ ℙ(Action)

Action = {Disclose, Deny}

Event = {RequestTo, RequestFrom}

Restriction = WeeklyPattern U User U Group U LocationPattern

Group = ℙ(Group, Network)

TimeSpan = [StartTime .. EndTime]

WeeklyPattern = ℙ(Weekdays) x TimeSpan

GeoArea = (xy_1, xy_2)

LocationPattern = ℙ(GeoArea)

3.1.3. Privacy policy management taxonomy

The privacy policy management taxonomy allows us to decompose the privacy policy management process into a set of basic operations over which we can perform restrictiveness accountability to be analyzed through time.

When users join Locaccino, the default privacy policies correspond to a null rule that enforces fail-safe defaults. This states that whatever event happens, the corresponding action always result in withhold at this stage. From then on, users can **create** rules, **add** restrictions to the existing rules, **modify** the restrictions, and **delete** existing rules restrictions and rules.

Restriction management actions can be of one of the following types:

- **Group-based restriction**: characterized by the users or networks that composes the group. For the sake of simplicity, we characterize this type of restriction according to the total number of elements of the group or network (*g_elem*). This variable is zero by default may take any non-negative integer value.
- **Time-based restriction**: characterized by its weekly time span. For the sake of simplicity, we characterize this type of restriction according to its total number of hours (*t_hours*). This variable is zero by default and range from zero to 168 hours.
- **Location-based restriction**: is characterized by a set of distinct locations (rectangles defined in Google Maps). For the sake of simplicity, we characterize this type of restriction according to the **total number of locations** (*l_number*). This variable is zero by default and can take any non-negative integer value.

It is likely that users use one rectangle for defining a location like “home” and another rectangle for “workplace”, while the respective areas may depend on many factors, e.g.,

the laziness of each user. Therefore the number of locations as a metric offers a good tradeoff between simplicity and meaningfulness.

Each privacy policy management action directly affects the variables defined above. The creation of a rule, depending on the restrictions that compose the rule, sets the corresponding variables (*n_elem* and/or *t_hours* and/or *l_number*).

Adding a restriction to an existing rule have a similar effect, but only the variable corresponding to the restriction being added is set (e.g., when a time-based restriction is added to an existing rule, *t_hours* is set).

The modification of a rule implies the modification of the variables corresponding to the restrictions being modified. For each restriction, the modification may increment the variable, decrement the variable, or the variable may even remain constant (e.g., a modification in a time-based rule that swaps 4 hours of location sharing from Monday to Tuesday).

The deletion of a rule sets all (*n_elem*, *t_hours*, *l_number)* variables to zero. The deletion of a specific restriction sets the corresponding specific variable to zero.

3.1.4. Restrictiveness

Restrictiveness is an intrinsic characteristic of restrictions associated to privacy policies (rules). It depends solely of the way the rule was defined. It does not depend of location requests or other events.

The relation between restrictiveness and the variables defined above depend solely on the type of restriction (social, time-based, location-based).

- **Group-based restrictiveness**: associated to a group-based restriction. We use the number of elements of a group (*n_elem*) as group restrictiveness metric (*GR*) provided with negative signal. Maximum restrictiveness corresponds to a group-based restriction with an empty group; group restrictiveness decreases with the addition of elements to the rule. In the limit, a group-based restriction with an infinite number of elements corresponds to zero restrictiveness, which is equivalent to not using group-based filtering at all.
- **Time-based restrictiveness**: associated to a time-based restriction. We use the total number of hours of sharing (*t_hours*) within a week as time restrictiveness metric (*TR*) provided with negative signal. Maximum restrictiveness corresponds to a time-based restriction with zero total hours of location sharing; minimum restrictiveness corresponds to the maximum number of hours of sharing (168).
- **Location-based restrictiveness**: associated to a location-based restriction. We use the number of shared locations (each defined by rectangular geographic regions in Google Maps) as location restrictiveness metric (*LR*) provided with negative signal. Maximum restrictiveness corresponds to a location-based restriction with no shared locations; location restrictiveness decreases with the addition of locations to the rule. In the limit, a location-based rule with infinite number of locations

corresponds to zero restrictiveness, which is equivalent to not using location-based filtering at all.

Rule restrictiveness is the restrictiveness associated to the combination of all existing restrictions (group-based, time-based and location-based) within a rule. Defining a metric for rule restrictiveness requires the use of normalized metrics for each of its components (restrictions). We denote the normalized restrictiveness metrics by *NGR*, *NTR*, *NLR*, referring to the normalized values of *GR*, *TR* and *LT* respectively.

Evaluating a rule is equivalent to intercept (*and()* function) the restrictions that compose the rule. Therefore, rule restrictiveness, *RR*, is defined as

$$RR = NGR \times NTR \times NLR$$

The normalization of time-based restrictiveness is the only case in which the operation is straightforward. We simply divide *TR* by the total number of hours within a week (168), obtaining *NTR*.

The normalization of group-based and location-based restrictiveness values can be done in several distinct ways. For group-based restrictiveness, we may divide GR by the user's social network size, obtaining the *NGR*. For location-based restrictiveness, we may divide *LR* by the total number of distinct locations travelled by a given user, obtaining the *LGR*.

Note that the normalization proposals for NGR and LGR above are not time-independent, since both user's social network and locations travelled may vary through time. Therefore, for analysis requiring time-independent restrictiveness metrics, alternative normalization solutions must be used.

3.1.5. Openness

Openness in the context of location-sharing can be defined according to diverse and distinct perspectives. We use a definition based on the disclose/deny ratio associated with the location requests targeted to a given user.

For example, consider a user whose location is requested 5 times at a given day. From these location requests only 2 are evaluated with disclosure. For the remaining 3 requests, the user is either hidden, offline, or the policy evaluates the request with "deny". In such situation, the user has openness 40% at that given day.

This openness definition is simple because it depends solely of the requests targeted to the user whose openness is being determined. However, strongly depends on the social network of a user. For instance, a user can raise/lower a friend's openness by repeatedly requests his/her location at a given time where the disclosure is known to be permitted/denied.

The simplicity of the our metric makes it simple to be implement and still provide enough information for the level of detail required in our experiment. We define the user openness more formally as follow.

Let *U* be the universe of users (user *A*, user *B*, user *C,* etc) and a given instant (day), *d*. The location requests performed by user *A* for user *C* are denoted by r_{AC1}, r_{AC2} .., r_{ACn}. Location requests can be divided according to their evaluation. More specifically, we denote the sets of all requests targeting user C which result disclosure, deny, hidden and offline evaluations as $r_C|disclosure$, $r_C|deny$, $r_C|hidden$, $r_C|offline$ respectively. We define the openness of user *C* for a given day, $OP_d(C)$, as

$$OP_d(C) = r_C|Disclosure \,/\, (r_C|deny + r_C|hidden + r_C|offline + r_C|disclosure)$$

3.1.6. Dynamic analysis of privacy policies

Our dynamic analysis decomposes a set of events over time, highlighting the ordering of these events, which may be important to understand cause-effect relations. We present one example of a dynamic privacy policies analysis as follow. Figure 1 illustrates the type of information that is highlighted in a the dynamic analysis (shadowed flanks, corresponding to the user's privacy policy modifications).

The upper part of the graphic represents the dynamics of the location requests and the respective openness. The requests represented here are the ones targeted to the user under analysis. The lower part of the graphic represents the dynamics of the privacy policy restrictiveness. The three types of restrictions (group-based, time-based, location-based) are represented in this lower part by the respective restrictiveness values.

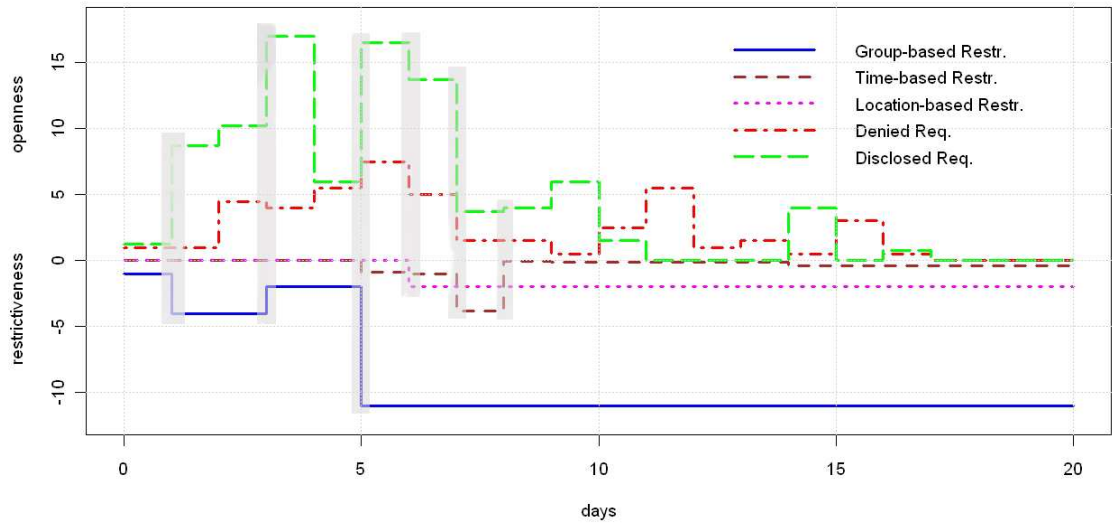

Figure 1 – Example of dynamic analysis of privacy policies

The privacy policy on the first day comprises at least one rule with at least one group restriction with 1 user. On the second day, the group-based restrictiveness decreased, meaning that either a new group-based restriction was added to an existing rule, or 3 users were added to the existing restriction. The resulting group-based restrictiveness is

4 at this stage. On the fourth day, the group-based restrictiveness raises to two (the restriction becomes more restrictive again). The user may simply have removed two elements from a group-based restriction, for example.

Several other privacy policy modifications occur throughout the twenty days of temporal analysis. What is important to emphasize in this example is that the goal of the dynamic analysis is to collect information about the user's privacy policy transitions (shaded areas).

Based on the dynamic analysis described above, we are interested in classifying users according to their privacy policy restrictiveness trend. The main goal of this classification is to understand if there is a generalized trend amongst Locaccino users.

The fact that Locaccino uses fail-safe defaults for privacy policies (i.e., default policies that have maximum restrictiveness) results that a first policy modification necessarily transforms the policy into a less restrictive policy. From then on, subsequent modifications can transform the policy into more restrictive or less restrictive.

We use the following **restrictiveness trend classification:**

- **Alternate**: Users that make several changes in their policies, making them more or less restrictive.
- **Constant**: Users that perform one unique modification in their policies or that perform policy modifications that do not affect the resulting restrictiveness.
- **Monotonic (decreasing)**: Users whose (all) policies modifications result less restrictive.

3.1.7. Feedback hypothesis

Time series with user's privacy policy restrictiveness and requests can be used for inferring the reasoning behind user privacy policy management, by looking for events in the vicinity of each rule modification that may have triggered the users' actions.

Locaccino users can observe the requests targeted them and the respective requests' evaluation. A description of this mechanism is provided in 3.3.1, where the Locaccino page "Who's Located Me" is scrutinized. In fact, for experimental reasons, some Locaccino were not provided with this functionality. However, we disqualified those users whenever necessary.

The feedback hypothesis states that the awareness (feedback) of location requests targeted to a give user (and respective evaluation) may trigger the decision to modify the privacy policy. Feedback can be used to support privacy policy management in two ways.

A negative feedback (denied location request), a user may modify the policy into a more open policy. On the other hand, the observation of accepted requests may trigger the modification of the policy into a more restrict policy as to protect the user from

undesired location disclosures. Note that both cases are denoted as the feedback hypothesis. Due to the simplicity of the model in use, the hypothesis is necessary but not sufficient.

More formally, the **feedback condition** implies that

1) At least a rule modification is preceded by denied/accepted location requests targeted to the user under analysis
2) the rule modification occurs within at most one day after the denied/accepted requests
3) that rule modification affects the restrictiveness
4) there is a direct effect on the user openness at most one day after that rule modification

The following figure illustrates an example of the feedback condition.

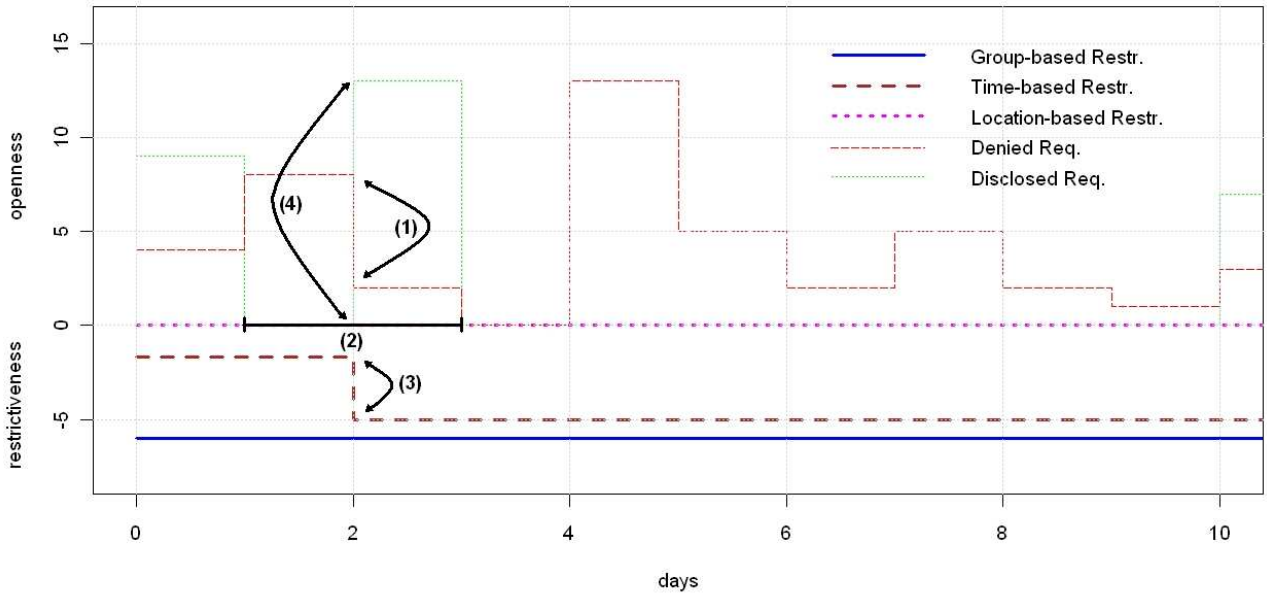

Figure 2 - Feedback condition illustration

In the example there are two instants with policy modifications, the first (1st day) with group and time-based restriction modifications, and the second (3rd day) with time-based restriction modification only.

The feedback condition is verified for the time-based restriction modification performed at the 3rd day. The four conditions are signaled in the figure, meaning that all of them occur for this policy modification.

3.2. Framework

3.2.1. Methodology

Several methods taken from social sciences have been adapted and employed for capturing generic user's feedback towards privacy. Two key factors decisively determine the potential bias in user's responses: user burden and situatedness [27]. The "cost" of each method is determined by its scalability, which is illustrated as follow.

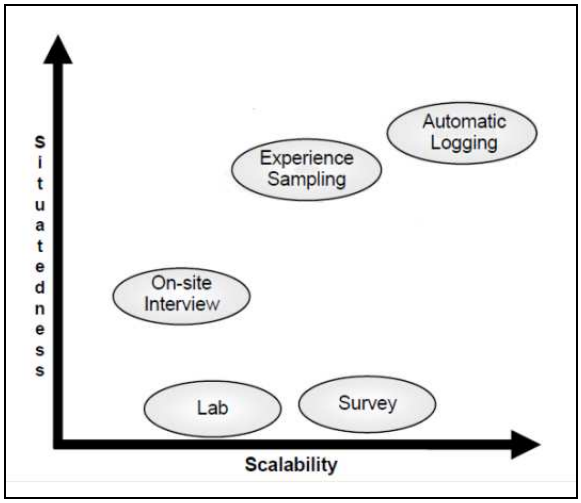

Figure 3 - Methods for capturing user's feedback

Surveys can have a bounded user burden, depending on the length and content, but are not adequate for capturing the feedback "in situ". Compared to the surveys, Experience Sampling Method [28] provides context to the users, thus, enhancing situatedness. Laboratory methods that simulate users' activity have reduced cost but are condemned to be artificial.

Usage data (automatic logging) is particularly suited for capturing the behavior of users when using an application because it is inherently "in situ". Moreover, it allows researchers to circumvent users' inaccurate perceptions of their own knowledge about privacy technology and vulnerabilities [29].

An additional strength of automatic logging, compared to traditional methods, is reproducibility: once developed, the framework can be used for other populations and studies. The adequate selection of the information (variables of interest) being logged and the respective logging rate determines the scalability of this method.

The framework developed in this project makes use of two studies that employ both surveys and automatic logging, thus, it can be seen as a hybrid method that results from the combination of automatic logging with surveys.

3.2.2. Dynamic analysis

Our framework allows analyzing through time the information collected from Locaccino database. Unlike in previous approaches, this type of analysis takes into consideration

the temporal dimension and the ordering of events and is expected to reveal aspects in user's behavior that would otherwise remain unrevealed.

The dynamic analysis of user's privacy policy management and location requests require some prior design decisions. Examples of such design decisions are the temporal window size, temporal granularity and time alignment.

Temporal window size

It is handy to define a fixed window size in order to be able to scale in our analysis. By limiting the analysis to the same temporal window for all users, we can analyze a group of users with certain characteristics or even an entire population.

This design option involves the following tradeoff: an excessively restricting the window size might lead to missing relevant data, however, long duration studies may become too expensive.

In our project we use an initial (conservative) temporal window size of 300 days. Using this initial window size, we determine a more practical value based on the analysis of the population of Locaccino users.

Temporal granularity

The choice of the temporal granularity strongly depends on the type of events to be analyzed. It could seem that the finer granularity the better, however, such approach can result in excess of information, resulting in missing the "big picture".

We use daily time granularity in our analysis. Moreover, we filter rule modifications that occur within short time periods because this kind of user behavior typically has to do with usability issues (user making mistakes while defining the privacy policy).

Time alignment

There are basically two options regarding time alignment in the temporal analysis: aligning or not. Time alignment must be performed if the topic of research is relative time (in opposition to global time).

An absolute time analysis could be interesting in case of knowledge of external events to be correlated with privacy policies modifications. For example, we could analyze the connection between large scale events (e.g., Independence Day) with user behavior patterns.

In our project, we use relative time. For each user the temporal analysis begins in the day of joining Locaccino and ends in the end of the study. We assume that no significant external events occurred that could induce biases to our analysis.

3.3. Locaccino

Locaccino is an application developed by the Carnegie Mellon's Mobile Commerce Laboratory in collaboration with CUPS, as part of the university's User-Controllable

Security and Privacy project [30]. It is intended to better understand people's privacy preferences in the context of location-sharing.

Locaccino is comprised of two main components: the web application and the locator (client) software. Several locators exist, since this software is device and OS specific.

The web application has user interface available as Facebook [31] application, which is convenient for reusing users' existing social network. This is where users can define and refine their privacy policies (rules), request their friend's locations and make use of some additional features.

The locator is the component of the software that is device and OS dependent. Users can install the locator on their laptops or on their smartphones. The software transmits the user's location to the Locaccino database every five to ten minutes [24] and provides the user with some controls (e.g., becoming invisible).

The Locaccino database stores locations of users transmitted by the locator software and also usage data, e.g., the location requests and privacy policy modifications.

3.3.1. Web application

The web application is divided into four main areas: "Home", "Privacy Settings", "Who Can Locate Me" and "Who's Located Me".

Home

The first area, "Home", is where the user can see his/her Facebook friends that are also Locaccino users. The user can then request their location individually or request the location of all friends within a certain range of proximity, with the "Show friends" feature.

Additionally, the user can request his/her own location, see some recommendations, and define settings related to Google Maps ("Map", "Satellite", "Hybrid", "Terrain").

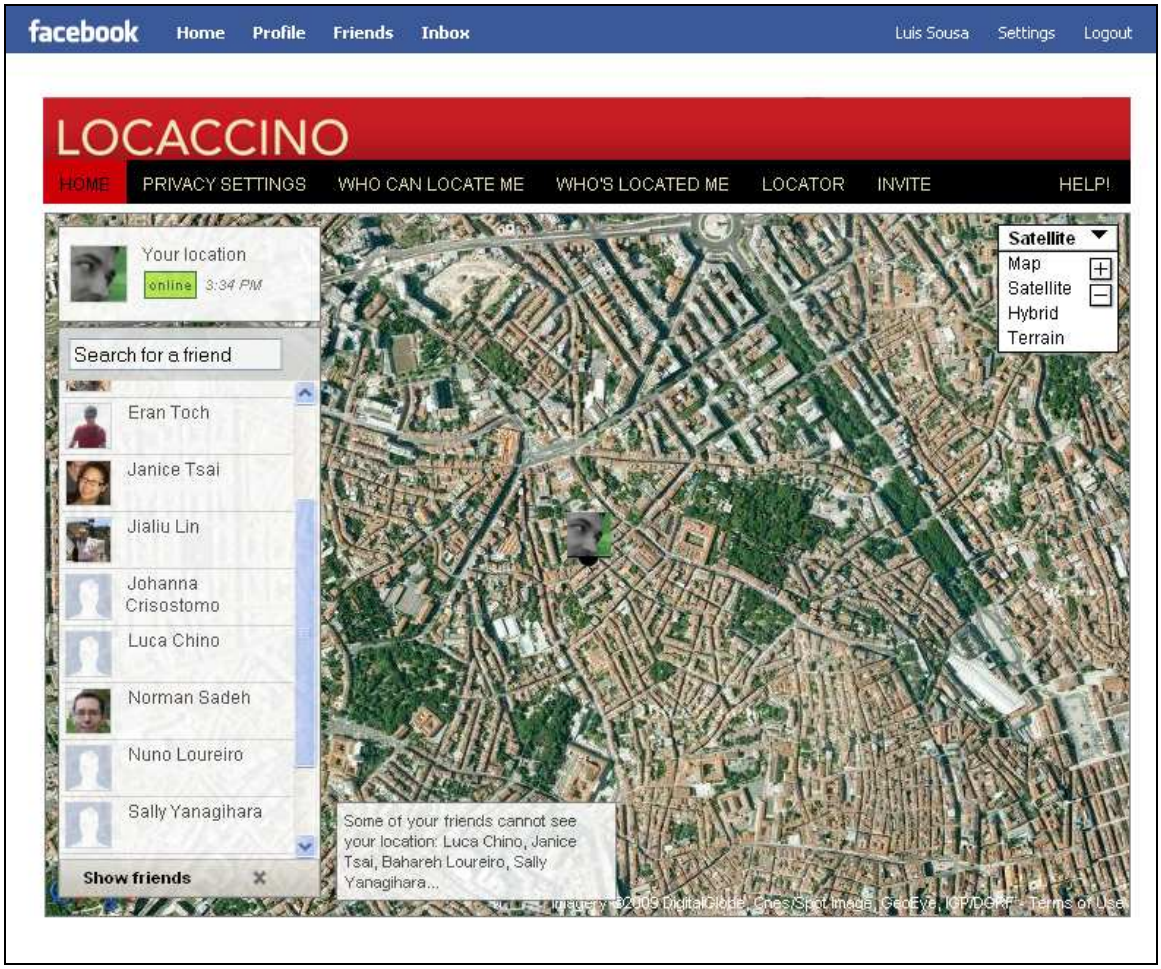

Figure 4 – Locaccino home page

Privacy Settings

This page is where the user can define the privacy policies that determine who, when and where can other users see his/her locations. In other words, in the privacy settings page the user can create, edit and delete the rules that serve as the basis for access control of location disclosure. Rules may be based in any combination of three types of restrictions:

- **Group-based restrictions**: define who can see the user's locations. It applies either to individual Facebook friends or entire networks of users with something in common.
- **Time-based restrictions**: define when the user's location can be disclosed. It is defined in terms of weekdays and time spans with granularity of half hours.
- **Location**-based restrictions: define the geographical area (rectangles in Google Maps) where the location of the user can be disclosed.

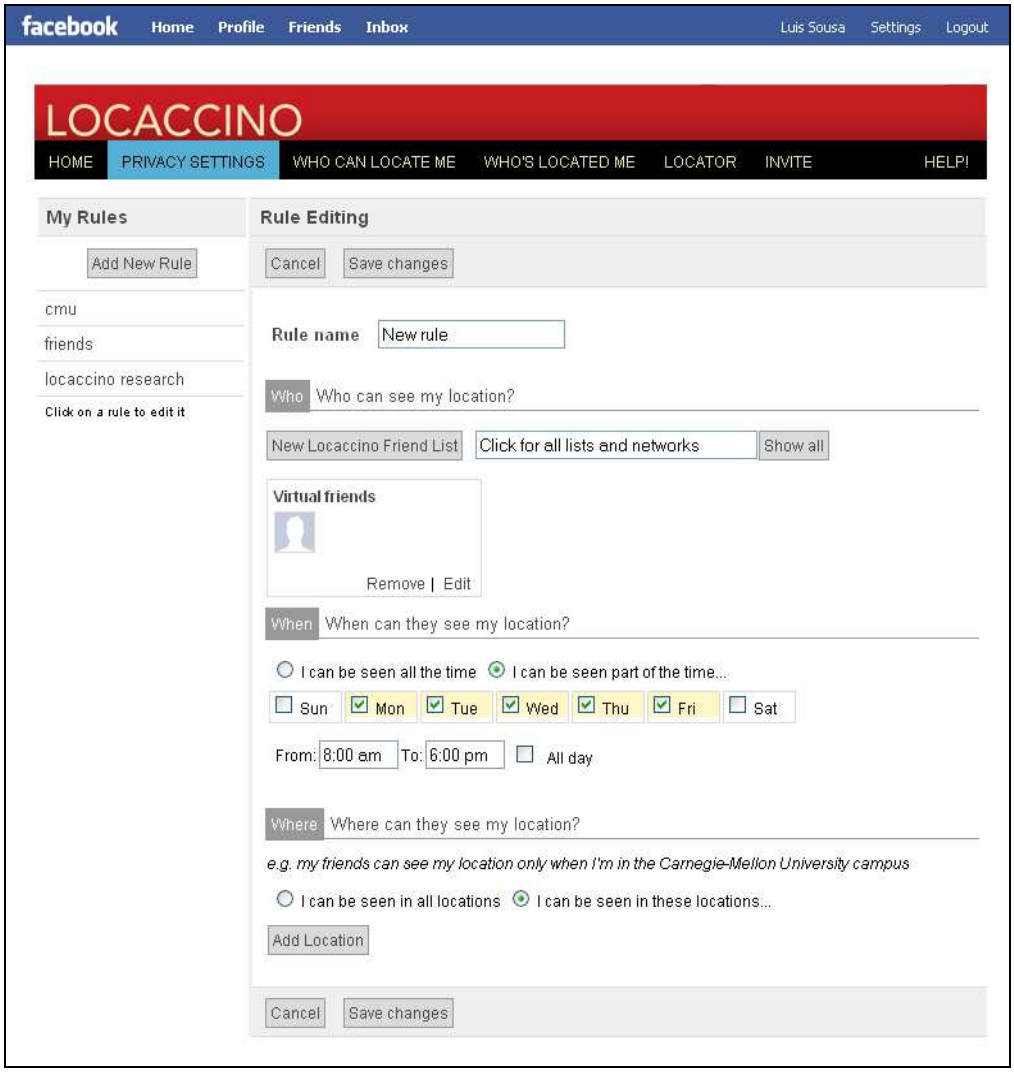

Figure 5 – Locaccino privacy settings page

We address in detail the topic of privacy policies, presenting the necessary formalism in section 3.1.2.

Who Can Locate Me

This page is intended to provide privacy awareness to the user, in the sense that the user can see at a given instant and free of ambiguities, the result of restriction evaluation for the group of friends. This page is also important for allowing users to confirm and correct their privacy policies, i.e., to easily evaluate whether the rules are producing the desired results at a given instant in time.

The following figure illustrates this mechanism. The group of friends of the user is basically split into two categories: the ones that can view the user current location and the ones that cannot.

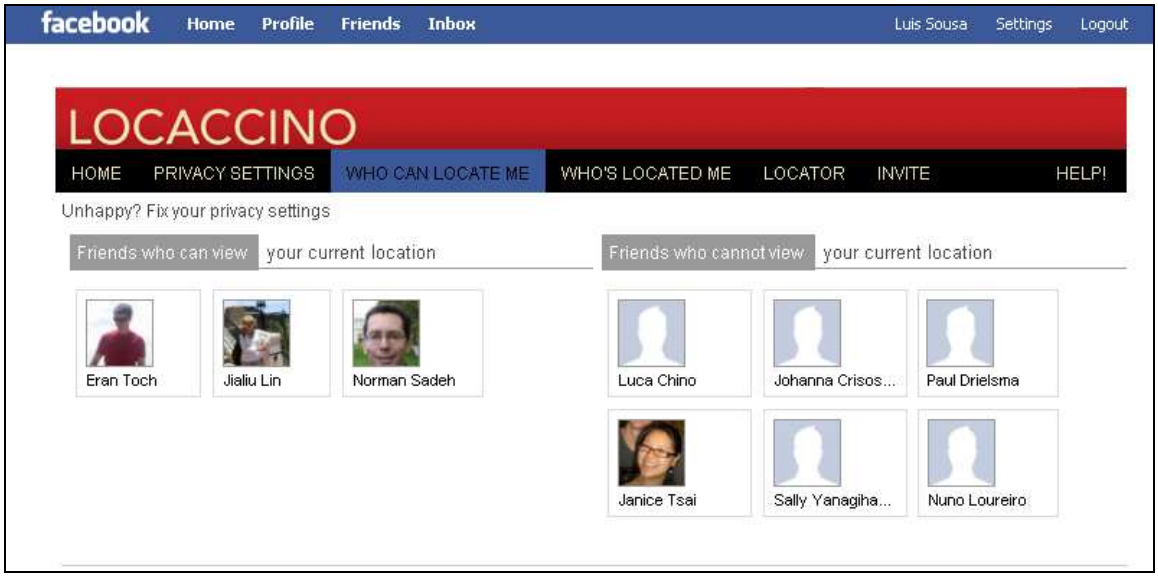

Figure 6 - Locaccino "Who can locate me" page

Who's Located Me

This page provides users with feedback about the friends that requested their location. There is a record for each request, with the requestor, timestamp of the request, location and address of the target user and the outcome of the request. The outcome results from the evaluation of the privacy policy of the target user for the specific location request and can be "Allow", "Deny", "Offline" or "Hidden".

This information is useful for deterrence, for helping users refine their rules, and also to provide audit information for research purposes. Users may provide a score in a *likert* scale referring to how comfortable they feel about each of the location requests. As referred before, this auditing mechanism has the strength of capturing "in situ" and in a contextualized fashion how comfortable users feel with each request. Figure 7 illustrates Locaccino "Who's Located Me" page.

3.3.2. Locators

There are currently two types of locators for Locaccino, targeted at laptop (Mac or Windows O.S.) computers and (Symbian O.S.) smartphones. Locators are installed on client machines and periodically send the machine's current location to the Locaccino server.

Wi-Fi positioning is the location mechanism used in laptop clients and in smartphone clients whenever GPS in unavailable. Wi-Fi positioning makes use of Skyhook (for generic locations) and CMU (specifically for the CMU campus) databases for correlating the access point information with the respective addresses. The smartphone locators also make use of GPS, which is the default location mechanism.

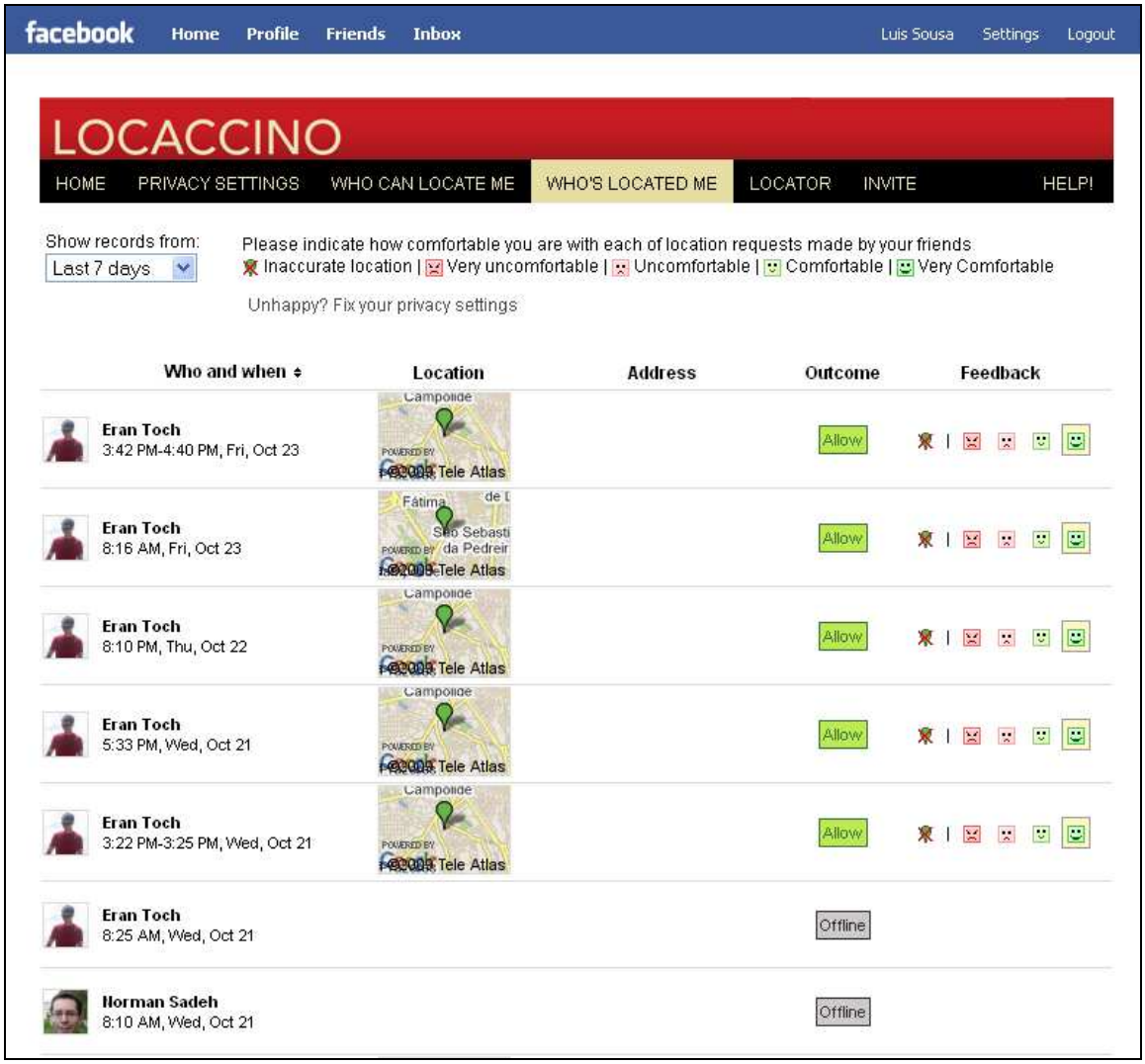

Figure 7 - Locaccino "Who's located me" (feedback) page

Additionally, the locator implements a small set of functionalities that are more or less limited depending on the type of device where the location is installed. The motivation behind these functionalities is to enhance the usability of Locaccino, by allowing the user to perform the most basic operations without requiring the access to Facebook. Examples of functionalities implemented in all locators are sign out/becoming invisible, and simplified versions of "Who's located me" and "Who can locate me".

Laptop locator

The laptop locator makes use of Wi-Fi positioning technology. Most Locaccino functionalities are implemented in the laptop locator, some of them in a simplified format for usability reasons. The definition of the privacy policies is the main exception, which requires the use of the Web application. The functionalities available in the laptop locator are illustrated in the following figure.

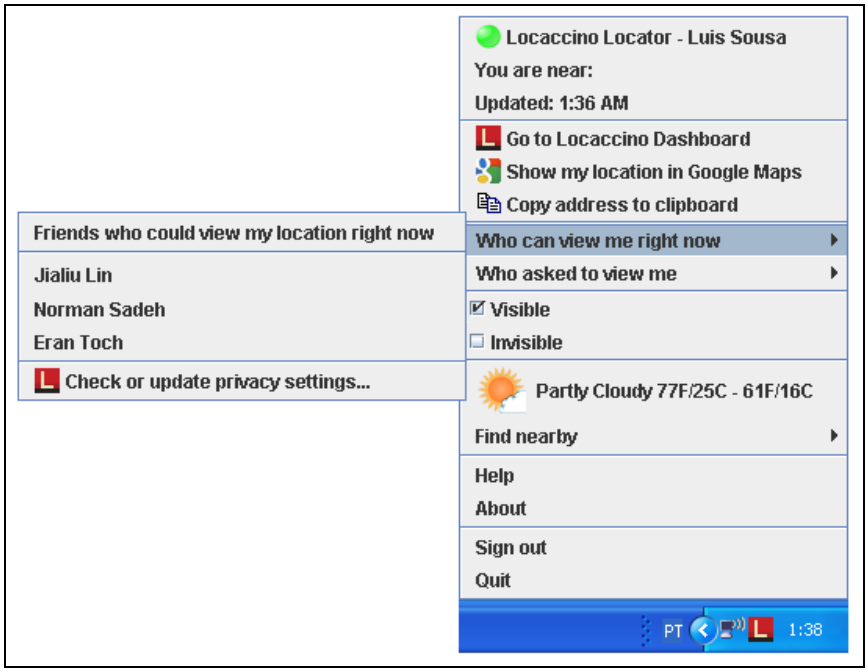

Figure 8 – Laptop locator (Windows OS)

Mobile locator

The mobile client was developed for the Symbian mobile OS and has been extensively tested on the Nokia N95 [24]. The mechanisms used for tracking the user's location are Wi-Fi or GPS positioning. The locator determines at any instant which of the two mechanisms to use depending of which one is available. In case both are available, it chooses the one that minimizes the power consumption. The GSM triangulation is still not implemented in this locator.

Examples of functionalities that, unlike in the laptop client, are present in the mobile client are the "Show Friends" functionality and the friends list. The following figure illustrates the "Show friends" functionality on the Nokia N95.

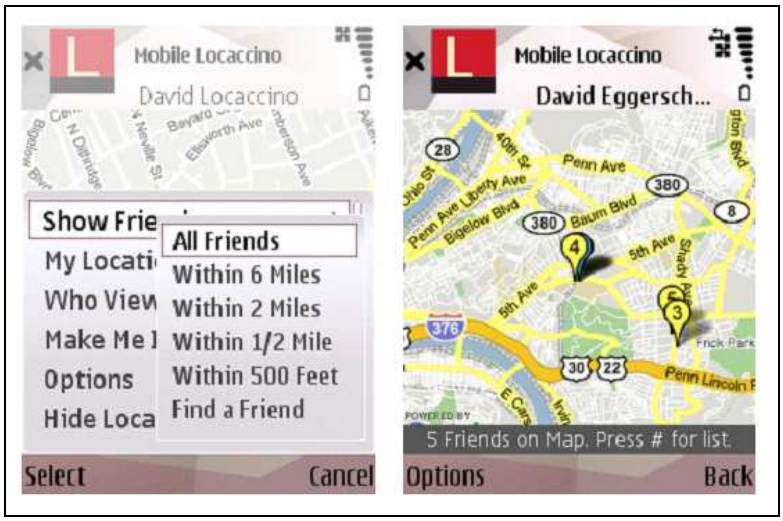

Figure 9 – Mobile locator

3.4. Experiment

We analyze two studies: long-term users study and mobile study.

One initial goal of the long-term users study is to find generic parameters to be used as rule of thumb in studies based on dynamic analysis for location-sharing applications. Examples of such parameters are the temporal window of analysis, the number of expected critical instants in user's privacy policy modification, and the time-to-converge of user's privacy policies. The mobile result is specifically focused in a closely analyze a comparison of laptop and smartphone users.

Both studies have some known limitations. In the long term-study, users experienced Locaccino possibly with distinct versions, meaning that they may have experienced minor differences in the functionalities implemented. They also might have experienced distinct recruitment methodologies: some may have been participants of field studies, while others may spontaneously have added Locaccino application in Facebook.

The mobile study has a small sized population (n = 28). The main reason for this was that the field study took place in the university environment during the summer, when most students are on vacations.

3.4.1. Long-term users study

This study involves the analysis of the Locaccino users whose activity duration is longer than one month (31 days). The reasoning behind this criterion is to select users that had enough time to change their privacy policies and were locatable through a long enough period to have an incentive to change their privacy policies.

We query the Locaccino user database using as main criterion the difference between the lowest and highest user timestamps in the system. We subtract to this group of 261 users the ones that participated in studies with hidden functionalities, e.g., users that were not provided with the feedback functionality. By disqualifying these users we ensure that the whole sample is provided with similar user interface, except for minor details.

Nevertheless, the group of 28 users that was not provided with the feedback functionality is used as a control group specifically for the validation of our feedback hypothesis.

Users that never modified their privacy policy are also disqualified since they do not provide information of interest for our project. The resulting group of users is denoted by "long-term users".

The policy management actions and the requests corresponding to these 144 users are the subject of our analysis. We exclude self-requests from this analysis because this type of requests belong to a distinct human behavior paradigm than the one that is subject of analysis.

Figure 10 and Table 2 characterize the sample in terms of the period of time in which the users were active in Locaccino. The six leftmost bars of the histogram correspond to the users that do not match the long-term criterion. All other users are considered to have long-term Locaccino experience.

Mean	48
Standard Deviation	56
Median	30
3rd Quartile	69
Maximum	256

Table 2 – Activity time period for long-term users

Users from this study resulted from distinct recruitment methods: some joined Locaccino spontaneously, others received the incentives of a specific field study and others were invited by study users.

Users may also have experienced different versions of Locaccino, which can result in potential sources of bias in our analysis. Therefore, this study is intended to provide generic insights.

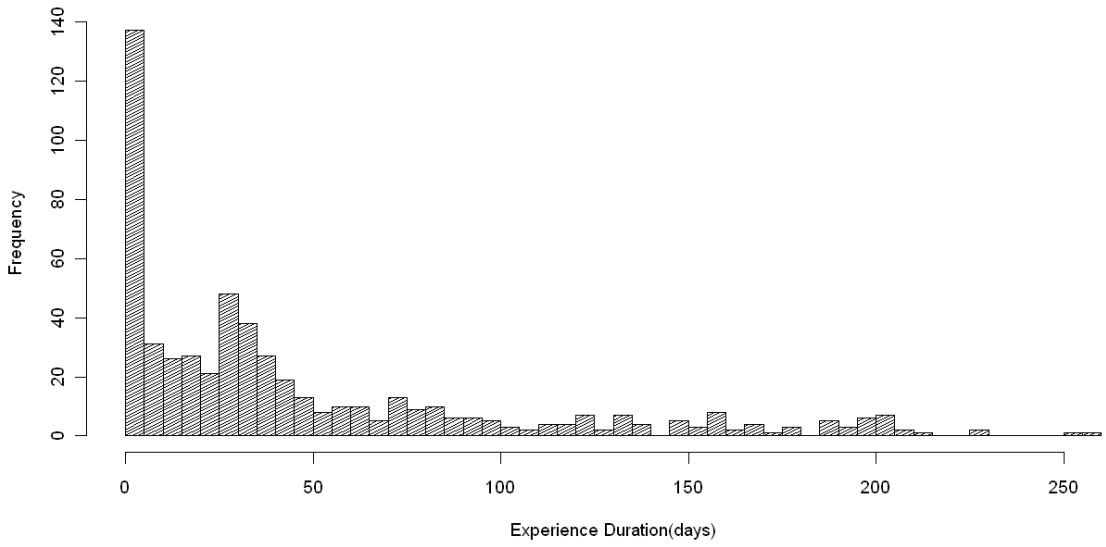

Figure 10 – Locaccino user's experience duration

3.4.2. Mobile study

This one month field study was intended to investigate the impact of mobility on location sharing. Participants of this study were recruited from the Carnegie Mellon University population using fliers and posts on electronic message boards. Participants were compensated $30 for their participation in the study. Participation consisted of four phases: the pre-study, the installation of Locaccino, Locaccino utilization and the post-study survey.

Pre-study

In the pre-study, potential participants completed a questionnaire that was used to evaluate their eligibility. Eligibility requirements included

- University membership
- Being user of Facebook
- Regular use of a laptop or smartphone
- Being current customers of AT&T or T-Mobile cellular services (necessary for the operation of the smartphone locator)

Additional questions were included in the pre-study survey regarding the potential users' technical expertise, demographics and attitudes towards privacy. Eligible participants were randomly assigned to one of the two **conditions**:

- laptop users (n = 11)
- smartphone users (n = 17)

Installation phase

The installation phase consisted in the installation of the Locaccino Facebook application and the locator client (described in sections 3.3.1 and 3.3.2 respectively). While laptop participants simply installed the locator client in their laptops (Windows or Linux OS), smartphone participants installed the mobile locator client on their provided Nokia N95.

Smartphone users were instructed to use the provided Nokia N95 as their primary phone, installing their personal SIM card phone. They were also required to have an active data communication plan, for which they were compensated an additional $15 for their data usage.

Utilization phase

Participants used Locaccino for a period of (at least) 4 weeks. Laptop users were instructed to have the locator running for at least an average of 5 daily hours. Using the provided Nokia N95 as their primary phone was considered sufficient for ensuring a minimum level of activity for smartphone users.

All participants were asked to audit location requests 3 times a week on non-consecutive days. Whenever the instructions were not followed for more than 2 days, users were reminded by e-mail.

After the 4 weeks of utilization, participants were asked to fill an exit survey. Smartphone participants returned their Nokia N95 phones.

Post-study

In the post-study survey, participants were asked about location privacy according to their 4 weeks experiences. First, they were asked to rate their comfort levels with sharing 12 specific locations with 5 social groups:

- Immediate family
- Close friends
- Acquaintances

- Anyone from the university population
- Everybody

The 12 specific locations were randomly sampled from among each user's locations travelled. For the (laptop) participants that were not observed in 12 distinct locations, all the distinct locations were asked to be rated. A *likert* 4-point scale was used, ranging from *very uncomfortable* (1) to *very comfortable* (4). Its phrasing and presentation were very similar to the auditing interface described in section 3.3.1.

Most participants that dropped out did so before the installation phase. Only 6 participants dropped out during the utilization phase, 3 in each group.

Data analysis

Our motivation in analyzing the usage data of this study is to analyze the user's privacy policy management through time. We also analyze the dynamics of the user's location requests to provide context awareness.

We removed the self requests from our data, which correspond to 31.5% of the total requests, because we are interested uniquely in requests that have privacy threat potential. We confirmed that all users had the feedback functionality enabled.

We analyze users without the feedback functionality uniquely for the validation of our feedback hypothesis on the long-terms users. The group of users without feedback enabled is used for control.

4 Results

The analysis of the data collected in the two experiments, described in 3.4.1 and 3.4.2, conducted to the results presented in the next two sections respectively.

For each study we provide results based on a static analysis of the location requests and privacy policy management process. Then, we provide the results of the respective dynamic analysis. Finally, based on the dynamic analysis, we analyze the hypothesis of the policy management process being influenced by the feedback observation.

4.1. Long-term users study results

One initial goal of the long-term users study is to find generic parameters to be used as rule of thumb in dynamic analysis studies for location-sharing applications. Examples of such parameters are the temporal window of analysis, the number of expected critical instants in user's privacy policy modification, and the time-to-converge of user's privacy policies.

After a brief characterization of the Locaccino long-term users, we move to the static and dynamic analysis in respect to users' privacy policy management and location requests.

4.1.1. Experiment design parameters

In this section we derive temporal design parameters, based on the observation of the temporal windows of user's generic activity. Note that any user-triggered event that is time stamped by Locaccino (e.g., location requests) is considered as generic activity in this context. We determine the number of days of Locaccino activity for each user and observe users' distribution in respect to this parameter.

We then repeat the same procedure for activities uniquely related to privacy policy management. Figure 11 allows comparing the resulting temporal differences for generic activity and privacy policy management.

Most users' activity lasts around hundred days. However, the number of users whose activity lasts between 100 and 200 days is non-negligible. This contrasts with the privacy policy management distribution, in which users typically define their privacy policies within a much shorter temporal window. Policy changes obey a power law distribution, where most users make the majority of the privacy policy modifications at the first days of usage.

Table 3 contains the resume of the temporal parameters of interest. Columns time of first change, time of last change and time duration have values in number of days. Time

duration is the time difference between the days of the first and last change. For this calculation we considered only users with more than one change.

On average, the first policy modification occurs on the 9th day of a user's Locaccino experience, while the last one occurs at the 17th day. Based on Table 3, our suggestion for the approximate observation period is the 3rd quartile of the fist policy modification added to the 3rd quartile of the privacy policy management window, calculated for the users that performed more than one policy modification. This results in the approximate value of 45 days (6 weeks).

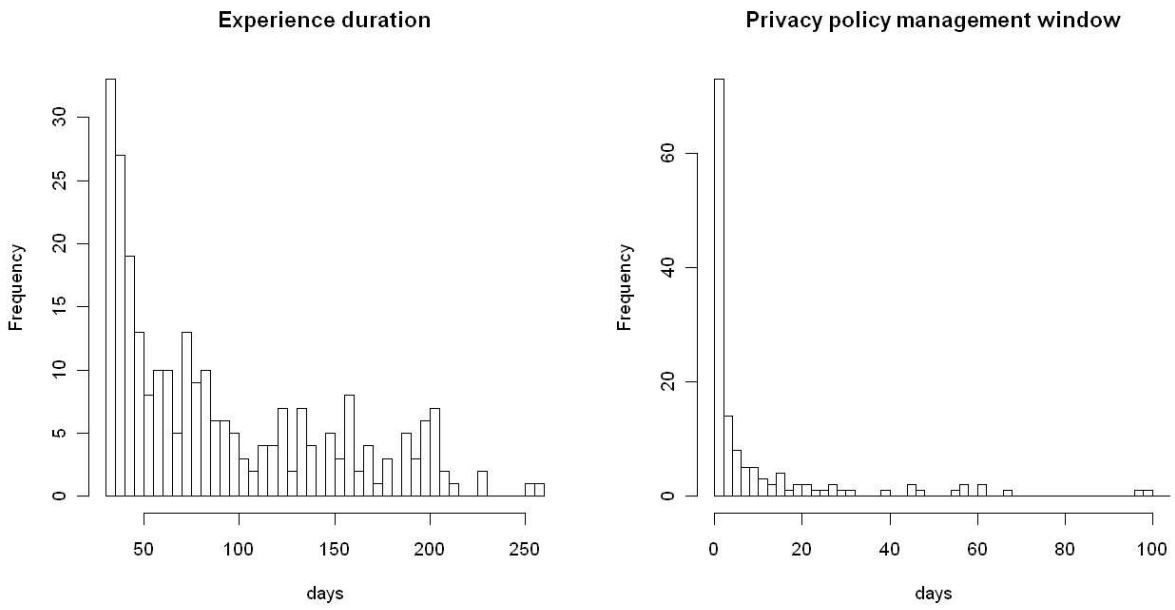

Figure 11 – Time duration of Locaccino user's activity

	Time of first change	Time of last change	Number of changes	Time duration (*)
Mean	8.8	16.6	1.5	31.1
Standard Deviation	24	34.8	1.2	42
Median	1	2	1	7.5
3rd Quartile	4	12.5	1.2	42.2
Minimum	1	1	1	1
Maximum	226	226	9	133

Table 3 – Privacy policy management parameters' characterization

4.1.2. Static analysis

This section is intended to characterize the population of Locaccino long-term users, based on descriptive statistics. This generic (static) characterization may be seen as the abutments over which lies the forthcoming dynamic analysis.

Location requests and openness

Table 4 provides the characterization of the long-term users' population in terms of location requests (performed by and targeted to) and the respective evaluation (openness).

Number of requests per requestor	146
Number of requests per target	111
Total number of requests	65493
Proportion of denied requests	8.5%
Proportion of hidden requests	4.3%
Proportion of offline requests	58.5%
Proportion of disclosed requests	28.8%

Table 4 – Long-term user's characterization in terms of location requests and openness

There is a clear asymmetry between requestor and target, meaning that, on average, users from this study typically perform more requests than the requests that are aimed to themselves. One justification for this asymmetry is the existence of the functionality "locate all" in Locaccino that allows users to locate multiple targets at once.

In terms of openness, the majority (58.5%) of the location requests are denied due to the fact that the user is offline. Apart from offline denied requests, most location requests result in disclosure (28.8% versus 12.8% of hidden plus requests denied by the users' policies).

Privacy policy management

We start by presenting the temporal characterization of users' privacy policy management, which is based on information from Table 3. We highlight the following observations:

- Long-term users modify their privacy policies at most in 9 distinct days
- Privacy policy time-to-converge of long-term users with more than one policy change is 1 month on average
- Only 5.5% of (long-term) users perform more than 2 privacy policy changes
- Only 25% of (long-term) users perform more than 1 privacy policy change

Table 5 provides the results from the analysis of the distribution of the privacy policy expressiveness and the respective restrictiveness. The three columns represent the distinct types of restrictions that compose the expressiveness spectrum.

Clearly, social (group-based) restrictions are the most used (45.3%). Additionally, the use of location-based restrictions for changing the privacy policy occurs on average around 3 days later than group and time-based restrictions. It is unclear whether this results from usability issues or if it is a user-intrinsic factor (users not interested in using this type of restrictions).

	Group	Time	Location
Restrictions distribution	45.3%	30.5%	24.2%
Day of use (mean)	24.5	23.9	27.1
Day of use (std)	44.7	43	46.5
Restrictiveness (mean)	-8.4	-49	-1.4
Restrictiveness (std)	13.5	41.4	0.5
Restrictiveness (min)	-140	-168	-3

Table 5 – Expressiveness (static) characterization of long-term users

Figure 12 and Figure 13 provide complementary information of group and time-based restrictiveness distributions, illustrating how users typically use these types of restrictions.

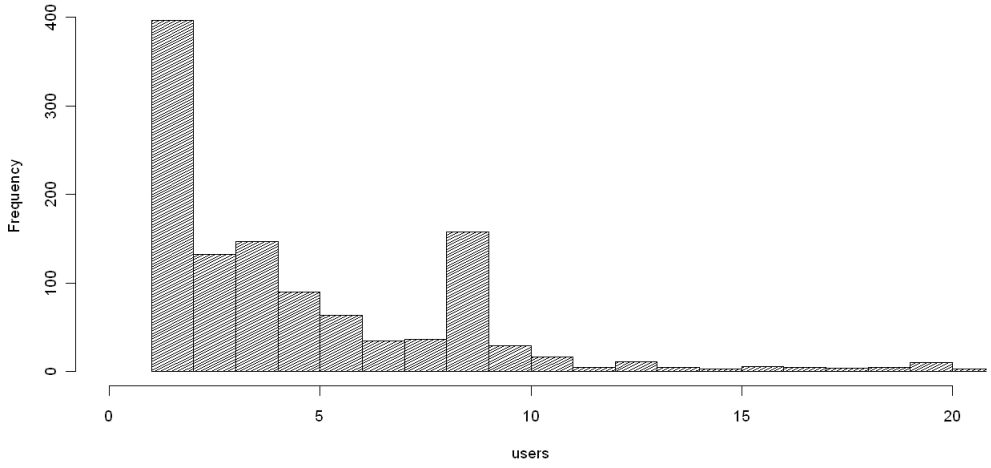

Figure 12 – Group-based restrictiveness distribution

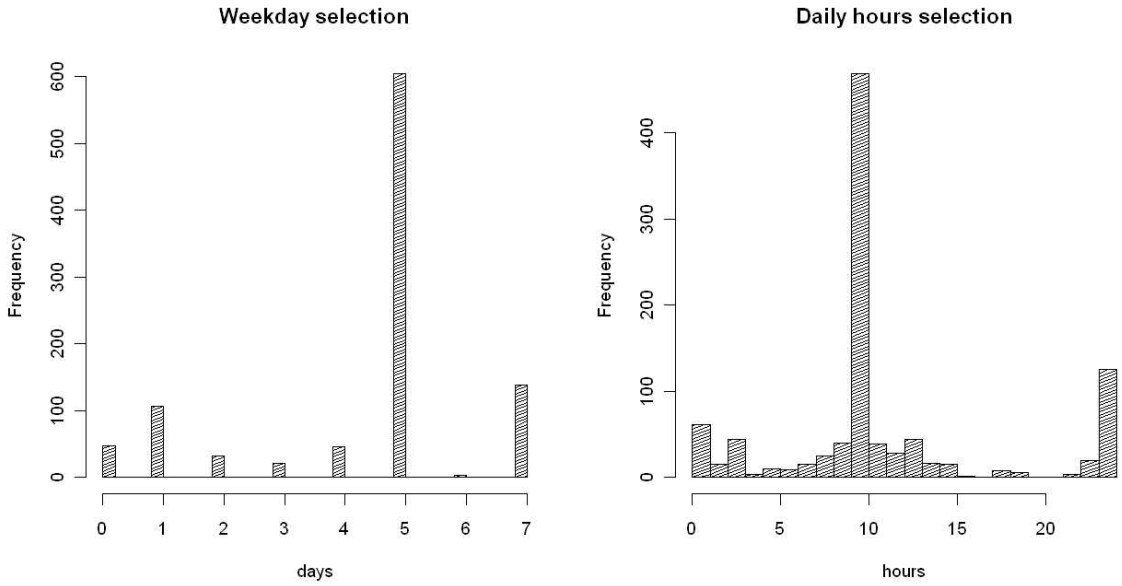

Figure 13 – Time-based restrictiveness distribution

We summarize the results from the static analysis of privacy policies restrictiveness as follow:

- **Group**: 8 is a popular choice for the number of elements for a group-based rule. This value results from mere empirical observation (Figure 12) and may be important for the design of highly constrained user interfaces (e.g., in mobile devices).
- **Time**: this type of restrictiveness is significantly biased by its default value, equivalent to 10 weekly hours of location sharing on weekdays (Figure 13).
- **Location**: the low number of locations used to address location-based restrictiveness suggests either the existence of usability issues for this specific type of restriction or people's lack of interest for this type of restriction.

4.1.3. Dynamic analysis

The dynamic analysis presented in this section focus on the evolution of location requests , privacy policy changes and openness through time. It includes the evaluation of user behavioral hypothesis (feedback hypothesis) in respect to the user's privacy policy management.

Location requests and openness

Firstly, we analyze the dynamics of the aggregate user's requests and respective openness. This aims at understanding the temporal distribution of the user activity of requesting other's locations and vice-versa. Figure 14 illustrates this for both locator and target perspectives. We use normalized values for the number of requests for an easier comparison.

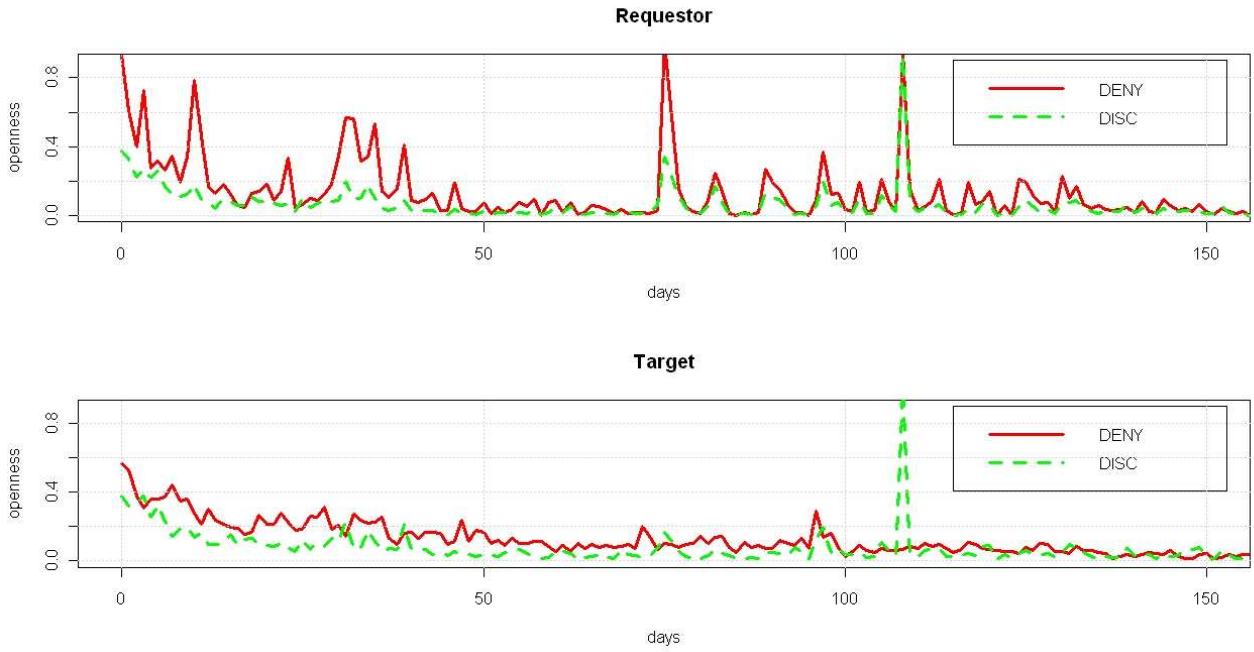

Figure 14 – Dynamics of long-term aggregate (all users) location requests

Our observations are:

- Despite the generalized initial decrement of requests, there is a lower bound on the location-request activity
- The level of denied (including offline and hidden) requests is consistently above the level of disclosed requests

Privacy policy management

There are two main goals in the dynamic analysis of privacy policy expressiveness: understanding if distinct types of restrictions are used in distinct times, and understanding users' evolution in terms of their use of expressiveness through time.

We expect users to become savvier in their privacy policy management process through time, however, it is not straightforward whether this evolution is visible within the observation temporal window in use.

Figure 15 illustrates the dynamics of expressiveness through the user's policy modification stage (iteration). The analysis is restricted to the first three policy iterations, since the number of users that have more than three changes is negligible. The percent values represent the distribution of each type of restriction in respect to the overall expressiveness.

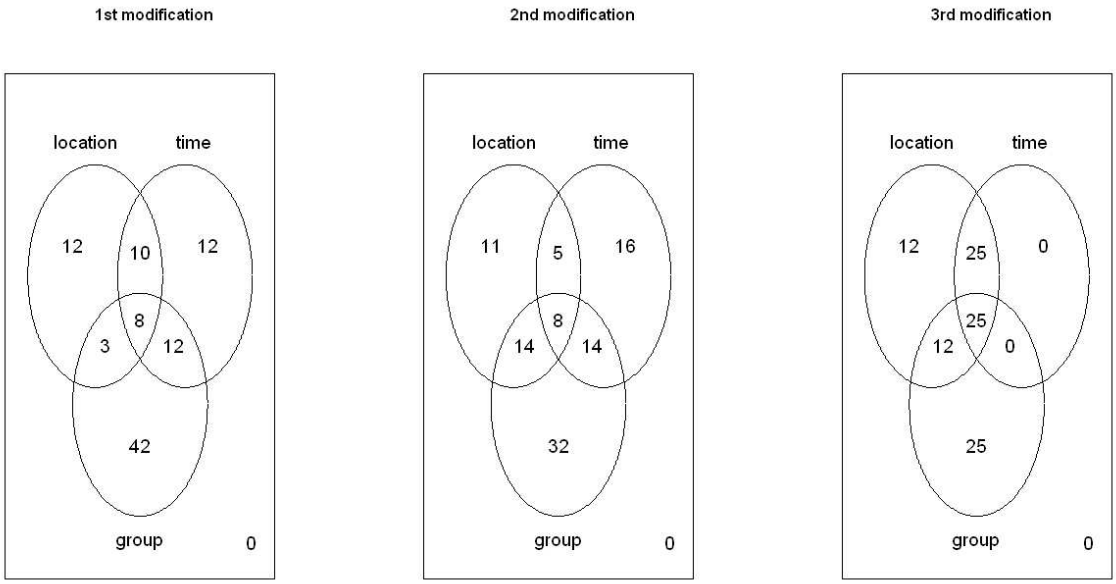

Figure 15 - Dynamics of privacy policy expressiveness (per iteration)

The main observations from this analysis are:

- The percentage of composite rules increases (33%, 41%, 62%) with the privacy policy modification stage, suggesting that users that perform more modifications in their policies also use a richer combination of restrictions in their later modifications.

- Modifications in rules affecting exclusively the group-based restrictions tend to decrease (42%, 32%, 25%) with the policy modification stage, compared to other restrictions.
- Time-based restrictions converge in just two policy iterations. This suggests that time, as a criteria for restricting one's location, is intrinsically more static than the social network or the locations travelled.

We follow with the classification of the users in terms of their privacy policy restrictiveness trend. The formal description of the privacy policy restrictiveness trend classification is provided in section 3.1.6. The population under study is distributed as follow:

- **Alternate restrictiveness**: Few users (3.5%) have this profile.
- **Constant restrictiveness:** Most users (75.7%) have this profile.
- **Monotonic (decreasing)**: 20.8% of users have this profile.

We notice that most users have a very passive attitude concerning their privacy policy. This is revealed by the fact that for most users, the restrictiveness remains constant after a first modification. More interestingly, we notice that the great majority of the remainder 74.3% users only modify the privacy policy making it more open (less restrict).

The following figure illustrates the privacy policy expressiveness distribution according to the trend profile. The percent values represent the distribution of each type of restriction in respect to the overall expressiveness.

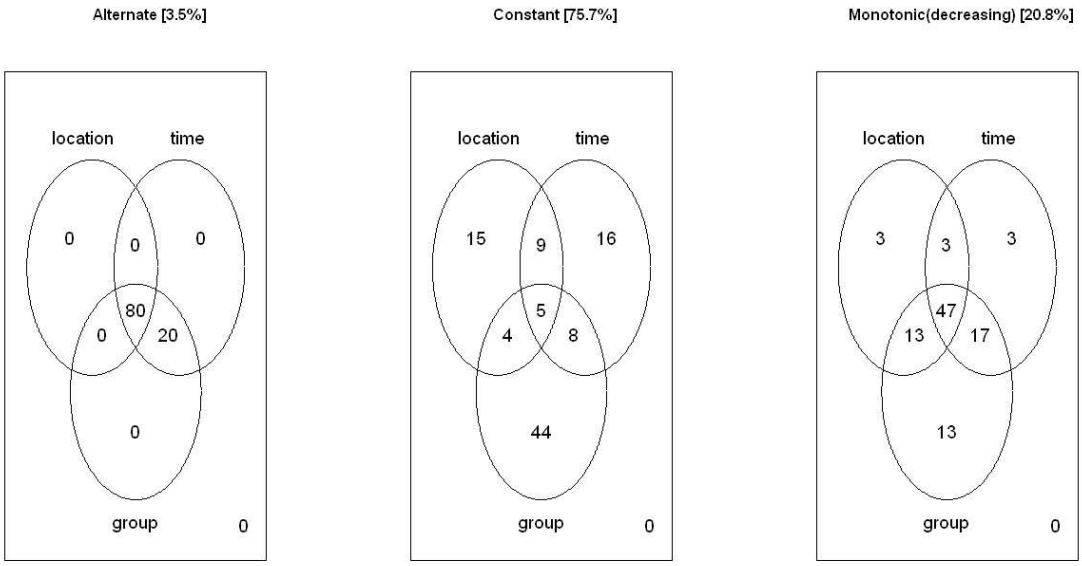

Figure 16 – Use of expressiveness according to privacy policy restrictiveness trend

The results from Figure 16 are aligned with the results from Figure 15. Users that modify their privacy policy only once tend to use less composite restrictions. Users with more privacy policy management iterations and making use of more types of restrictiveness modifications, also make use of more composite restrictions in their privacy policies.

Finally, we analyze the dynamics of the aggregated privacy policy restrictiveness. The use of normalized restrictiveness values provide the information of how the restrictiveness (of distinct types) decreases trough time, which is illustrated in Figure 17.

Prior analysis of Figure 15 revealed that the significance of group-based restrictions in the overall user's expressiveness tend to decrease. The aggregated cumulative restrictiveness analysis confirms this result. For example, on the 3rd day, users already used, on average, 72% of their group-based restrictiveness but only 53% of their time-based and location-based restrictiveness.

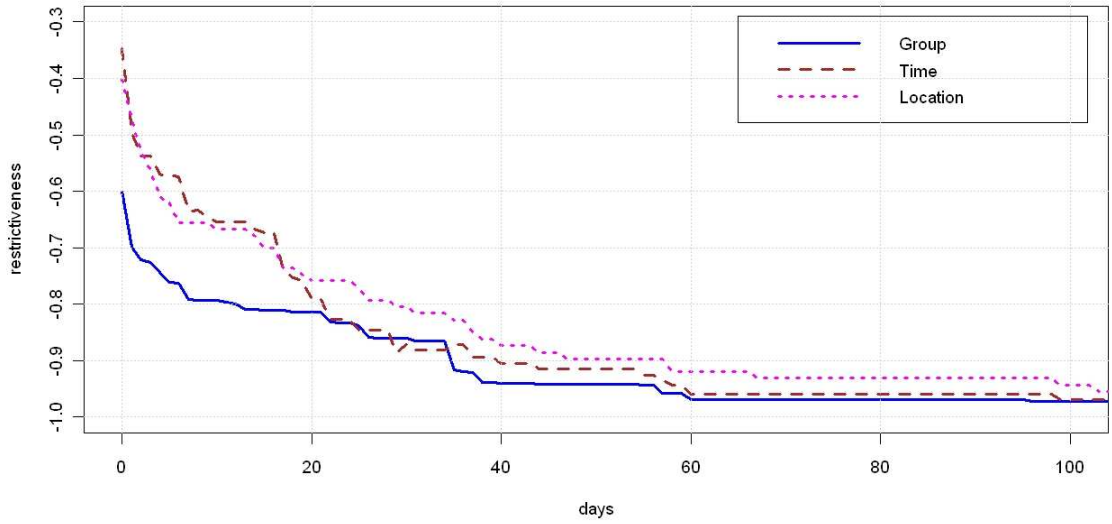

Figure 17 – Aggregated cumulative restrictiveness dynamics

Feedback hypothesis

In this section we evaluate the feedback hypothesis, presented in section 3.1.7. We evaluate the hypothesis in regard to users who had access to feedback and also for the ones that were not provided with feedback (control group).

Our results reveal that the feedback hypothesis holds true for 27.1% of the users that were provided with feedback and 17.9% for the ones that were not provided with feedback. Based on this analysis, feedback seems to have an important role, not only in users' privacy awareness, but also in users' privacy policy management.

The average number of policy modifications and the average time-to-converge of policies are also higher for the feedback group.

	Feedback	No Feedback
Feedback hypothesis	27.1%	17.9%
Group-based changes	68%	54%
Policy changes (mean)	1.45	1.29
Temporal window (mean)	31.2	15.7

Table 6 – Comparison between feedback and no-feedback groups (long-term users)

Additionally, we notice that privacy policy modifications that fall in the feedback-driven category typically involve a higher usage of group-based restrictions (62% for uncorrelated modifications versus 83% for users in the feedback condition).

Locaccino feedback page provides information of both locator, time of request and location of the target, i.e., it provides information that can be used for refining all the three types of restrictions. However, users seem to use more predominantly the locator information than the temporal and geographical contextual information for refining their privacy policies.

4.2. Mobile study results

The inclusion of the mobile study in this project has two main goals: to validate some results of 14.1 (which rely on sample not necessarily recruited under the same conditions) and to investigate the differences in privacy policy management when users are using Locaccino in their smartphones rather than (the most common scenario) in their laptops.

The results of the mobile study are presented in two distinct sections, the first for the static comparative analysis and the second for the dynamic comparative analysis.

4.2.1. Static analysis

In this section we provide a generic comparative characterization of the population being studied. This generic (static) characterization may be seen as the abutments over which lies the forthcoming dynamic analysis.

Location requests and openness

The location requests activity of users and the respective requests evaluation (openness) are presented in Table 7, according to the type of device. The *requestor* and *target* columns identify the device of the user that performs the location request and the user whose location is requested, respectively. We denote as “outside” the users (either requestor or target) that do not belong to the population of the study.

Requestor	Target	Number of Requests	Denied requests	Hidden requests	Offline requests	Disclosed requests
laptop	laptop	610	1,0%	3.0%	25.7%	70.3%
laptop	smartphone	56	0.0%	0.0%	30.4%	69.6%
laptop	Outside	226	9.7%	15.0%	54.9%	20.4%
smartphone	laptop	59	3.4%	25.4%	16.9%	54.2%
smartphone	smartphone	788	3.7%	1.4%	39.6%	55.3%
smartphone	Outside	1208	1.7%	2.3%	83.0%	13.0%
Outside	laptop	195	2.1%	25.1%	48.7%	24.1%
Outside	smartphone	468	18.2%	0.0%	26.5%	55.3%

Table 7 – Location requests and respective evaluation for laptop and smartphone users

In Table 8, we present the results that highlight the differences in the (aggregate) requests of laptop and smartphone users, as well as the respective openness.

The *requests by participant* column contain the total number of requests performed by participants specifically in the laptop/smartphone group. The *requests to participant* column contain the total number of requests performed to participants specifically in the laptop/smartphone group. The *openness of participants* column contains the average openness of participants according to their laptop/smartphone group.

Participant's device	Requests by participant	Requests to participant	Openness of participants
Laptop	44.6	43.2	49.60%
Smartphone	186.8	119.3	60.10%

Table 8 – Laptop versus smartphone user's comparative openness

We resume the analysis of the tables above in the following observations:

- Smartphone users perform more requests than laptop users (186.8 versus 44.6 requests per requestor user during the period of observation).
- Smartphone users' location is more requested (119.3 versus 43.2 requests per target user during the period of observation)
- Smartphone location disclose rate is also higher (60.1% versus 49.6% of the location requests were accepted).

The fact that the disclose rate values for this study are much higher than the ones obtained in 4.1 may find justification in the recently developed Locaccino functionality that allow users to know ahead of time which friends are locatable. Nevertheless, there is a weak relation between the mobility and the openness of users.

Privacy policy management

The temporal parameters of both smartphone and laptop policy management activity are presented in the following table. The first three rows of the table characterize the users in respect to their privacy policy modifications and the last row refers to (generic) policy modifications. All values refer to average number of days except the user's (average number of) policy modifications.

	Smartphone	Laptop	All
User's first policy modification	3	1.3	2
User's policy modifications	1.6	1.2	1.4
Temporal policy MGMT window	3.3	0.8	1.8
Generic policy modification	4.4	1.9	3.2

Table 9 – Privacy policy management temporal characterization

The differences between smartphone users and laptop users in respect to their privacy policy management temporal parameters are presented as follow.

- Smartphone users, on average, start modifying their privacy policies later.
- Smartphone users, on average, perform more policy modifications.
- Smartphone users, on average, make use of a larger temporal window for policy modification.
- Privacy policy modifications occur later on average for smartphone users. This temporal offset is of 2.7 days for the first modification and 3.3 for generic policy modifications.

Privacy policy expressiveness

A comparative analysis of the privacy policy expressiveness between laptop and smartphone users is provided in the following figure. The percent values represent the distribution of each type of restriction in respect to the overall expressiveness.

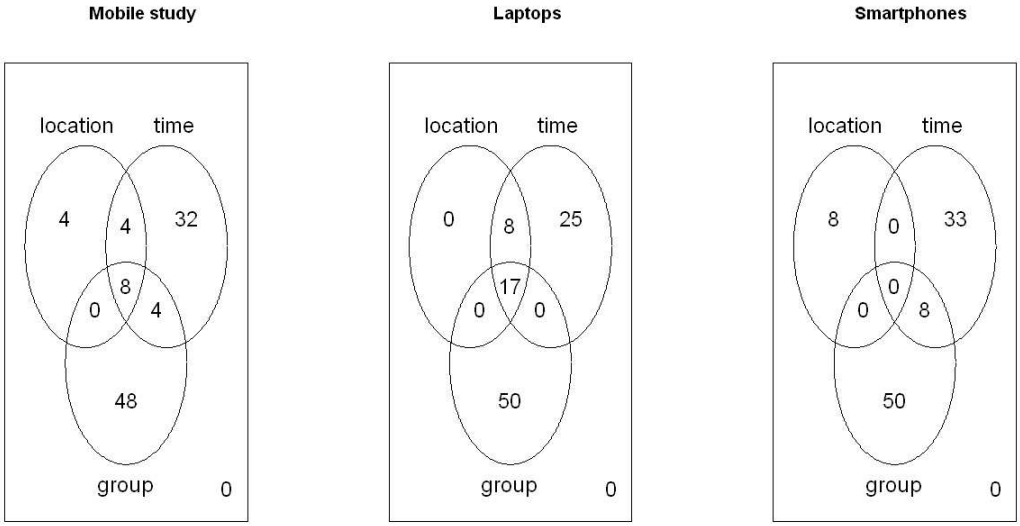

Figure 18 – Privacy policy expressiveness distribution for laptop and smartphone users

The most relevant differences between smartphone and laptop users in respect to their privacy policy expressiveness are:

- Smartphone users use less combined restrictions. This may be related to usability issues specific of the mobile interface or to the fact that the same usability issues have more negative impact in mobile platforms.

- Smartphone users make use of less location-based restrictiveness (8% versus 15%), which is odd, since these are the users that have a wider spectrum of locations to share/restrict.

4.2.2. Dynamic analysis

The dynamic analysis presented in this section focus on the evolution through time of location requests (and respective openness) and privacy policy management (and respective restrictiveness). The former includes the evaluation of user behavioral hypothesis in respect to the user's privacy policy management.

Location requests and openness

The analysis of the dynamics of the aggregate user's requests and respective openness aims at understanding the temporal distribution of the user activity of requesting other's locations and vice-versa. Figure 19 and Figure 20 illustrate, for laptop and smartphone users respectively, both the locator and target perspectives. We use normalized values for the requests values.

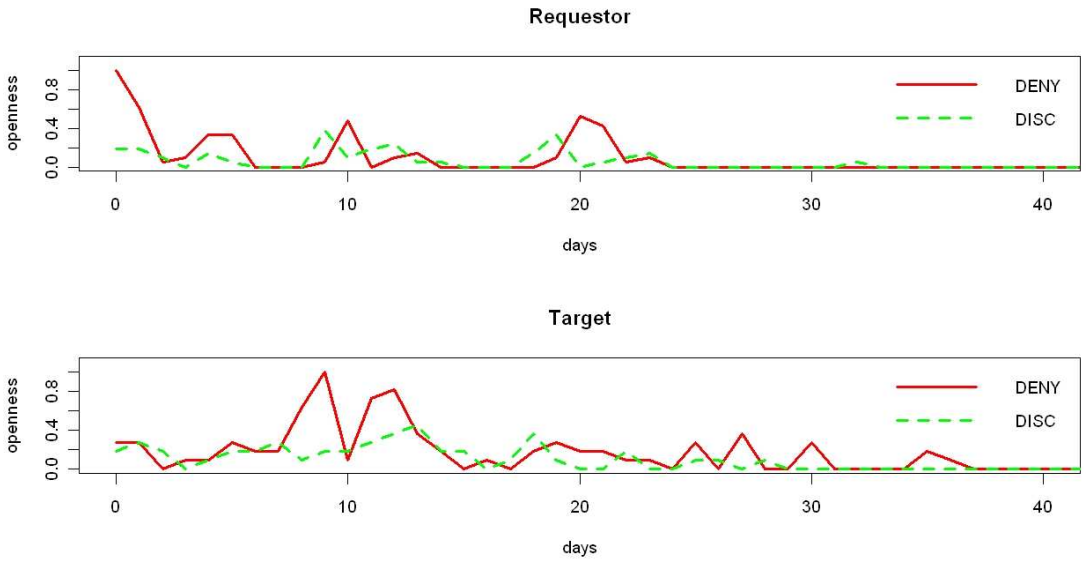

Figure 19 – Dynamics of laptop user's location requests

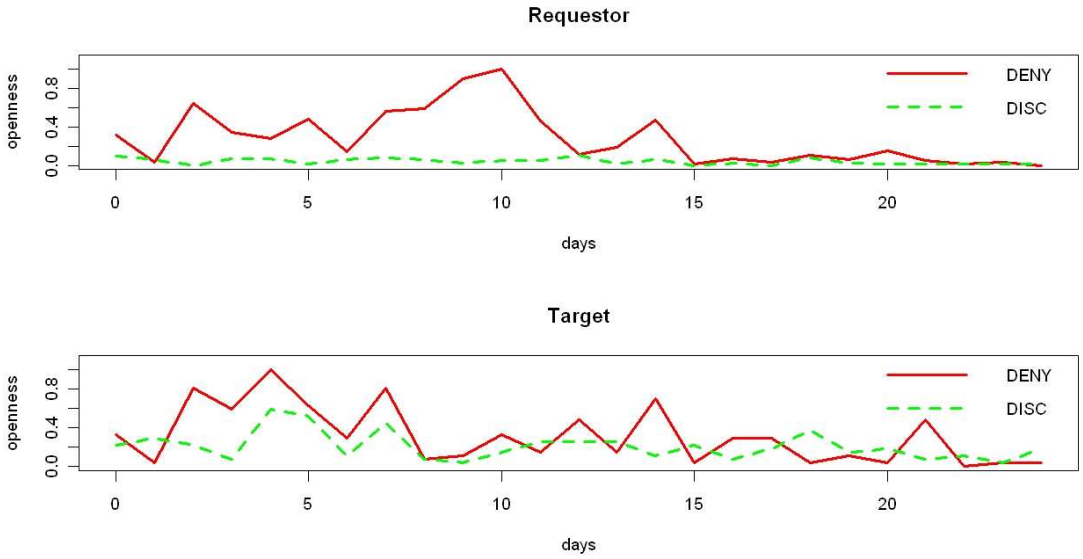

Figure 20 - Dynamics of smartphone user's location requests

The dynamics of laptop and smartphone user's location requests do not reveal significant differences. As previously noticed, there is a small (approximately 2 days) temporal offset of smartphone users, resulting from starting their activity slightly later than laptop users. The location requests of smartphone users are more concentrated (in contiguous time periods) than the requests of laptop users (more sparse).

Privacy policy management

The dynamic analysis of mobile user's privacy policy management is based in the aggregation of all users' policy restrictiveness according to the type of restriction. Figure 21, Figure 22 and Figure 23 illustrate the scenarios with all users of the mobile study, laptop users only, and smartphone users only (respectively).

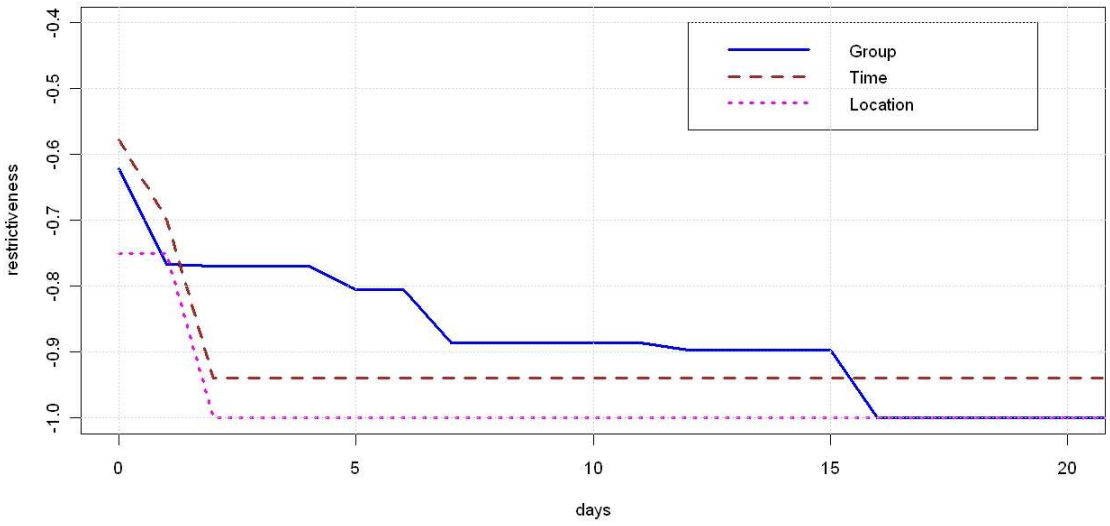

Figure 21 – Dynamics of mobile study user's aggregate (normalized) restrictiveness

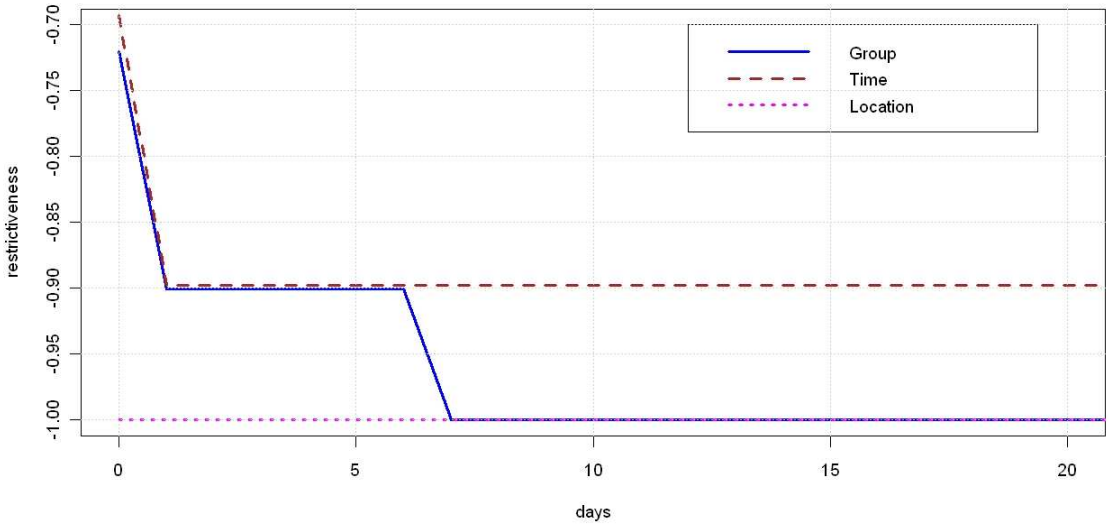

Figure 22 – Dynamics of laptop user's aggregate (normalized) restrictiveness

Users from the mobile study have a dynamic privacy policy pattern in which the time and location-based restrictiveness are rapidly applied (more than 90% is applied in the first 3 days), while the group-based restrictiveness is applied in a more gradual fashion. Nonetheless, after the 3 days of Locaccino experience, users applied 75% (for all types of restrictions) of all the restrictiveness they will use in their privacy policies.

The comparison of Figure 22 and Figure 23 reveals that laptop users are more prompt in applying their restrictiveness (more than 90% of all types of restrictiveness within the first 2 days) than smartphone users. Smartphone users were required 16 days for applying similar amount of restrictiveness.

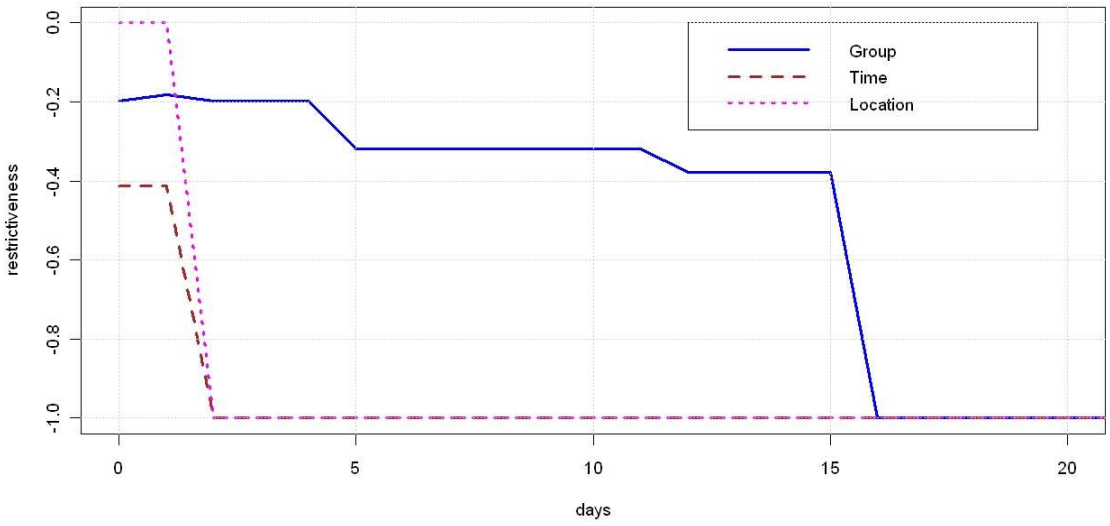

Figure 23 - Dynamics of smartphone user's aggregate (normalized) restrictiveness

The results of the dynamic analysis of the mobile users' privacy policy management are resumed as follow:

- Mobile users' dynamic privacy policy restrictiveness pattern differs from the pattern observed for long-term users. The main difference consists in whether users apply more rapidly their group-based restrictiveness or their time and location-based restrictiveness.
- Mobile users apply their time-based and location-based restrictiveness very rapidly (more than 90% within 3 days).
- Smartphone users take more time than laptop users to define their privacy policies. This is even more relevant for group-based restrictions.

Hypothesis for user privacy policy management behavior

In this section we evaluate the feedback hypothesis, presented in section 3.1.7. We evaluate the hypothesis in regard to users who had access to feedback. Because we do not have users from the mobile study without feedback functionality, we are forced to use a transitive reasoning. After concluding that the feedback hypothesis holds with higher probability for (laptop) users with feedback functionality, we then compare laptop users to smartphone users.

Interestingly, the probability of a privacy policy modification being connected to feedback is much higher for smartphone users (50% versus 7.7%). The value obtained for the whole population of the mobile study is consistent with the value obtained for the study of long-term users.

This analysis validates feedback as having an important role, not only in users' privacy awareness, but also in users' privacy policy management. Its importance is higher for smartphone users, whose privacy concerns are inherently higher.

5 Discussion

The results of this project, composed by two studies, impact the design of user interfaces for location-sharing applications and also future research on the same topic. Additionally, they provide relevant insights for understanding the evolution of the location-sharing paradigm.

5.1. Implications for design

The results of this project may impact several aspects of the design of user interfaces in location-sharing applications:

Privacy policy awareness

This study revealed the importance of the feedback functionality for helping users defining their policies, which is particularly noticeable for the smartphone users.

Complementary mechanisms for helping users evaluating the effectiveness of their privacy policies can also be implemented in the user interface. One such mechanism is the inclusion in the feedback of a reference to the rules that allow the disclosure of each location. Additionally, the interface should alert users of the rules that are never used and provide statistics about which rules are the most effective, friends that that request more locations, periods of the day, etc.

Machine learning techniques

The results of this study also revealed the user's privacy policy modifications become more complex over time. Machine learning techniques for helping the users in the process of privacy policy management must take this observation into account, by providing suggestions with increasing level of complexity/richness.

The dynamics of suggestions must also take into consideration that time-based restrictions are the most static, location-based restrictions tend to become more dynamic in the mobile scenario, and social-based restrictions have long-term dynamics.

User interfaces for mobile devices

Due to the inherent limitations of smartphone interfaces (e.g., reduced screen size), the prioritization of the functionalities is crucial for its selective inclusion in the user interface.

The interface component that allows the users to modify the privacy policies must include the minimum necessary information for the definition of the restrictions. For the group-based restrictions, we suggest forms optimized for (3x3) nine elements, since the results of the study demonstrated that most group-based restrictions have eight elements.

A tailored version of the feedback functionality must be implemented in the smartphone versions of Locaccino, where the information of the requests locator must prevail over the temporal and geographic contextual information.

5.2. Future work

Data from both long-term and mobile studies revealed some weaknesses by containing scarce information for dynamic privacy policy analysis. While some of these weaknesses are user-intrinsic, workarounds can be found for some.

In the user-intrinsic category, we find the generalized low level of usage of our location-sharing application, which is particularly critical in terms of privacy policy management. The increment in the activity observed in users with mobile devices suggests that, aligned with the adoption of location technology by the mobile market, data available for research in the near future will be necessarily richer.

We also found difficult to ensure with certainty, based on the existing data, that a given policy modification is related to an event, e.g., with the visualization of feedback. The existing auditing mechanisms are insufficient for this purpose because they are strongly dependent of the users, therefore, the logging of the user feedback visualizations should be collected as complement.

It remains an open question whether the lack of popularity of location-based restrictions is due to usability issues or to the fact that users find it unnecessary. We suggest stronger metrics for the analysis of location-based restrictiveness, e.g., combining characteristics of the locations defined in the rules with the actual user's location. Additionally, both smartphone and laptop users should be asked about this topic in a survey.

In this study, users typically performed short-term privacy policy modifications that resulted into more open policies. We believe that this monotonic behavior will change with the user savviness and the penetration of smartphones. Nevertheless, users should be asked whether the stability and monotonic behavior of their policies is due to the fact that users perceive their policies as efficient, or due to other factors.

5.3. Location-sharing evolution

The generic activity of location-sharing users provides a good metric for evaluating user's tradeoff between the location sharing benefits and the privacy concerns that these applications raise.

Our results suggest that mobile devices bring enhanced activity to the location-sharing scene. Compared to laptop users, smartphone users produce more location requests, receive more requests and are more open in general. In other words, smartphone users are more active, their locations are more valuable to the location-sharing community, and they are more open to sharing. Note that the fact that smartphone users are more

open is beneficial for the generalized adoption of location-sharing by reducing the risk of users having their locations requests systematic denied.

Mobile devices not only bring enhanced location-sharing activity but also raise additional privacy concerns to users. We believe that the impact of our results in the design of user interfaces result in significant enhancements in the way they address the privacy concerns that have been a barrier to the generalized adoption of location sharing applications.

The combination of the enhanced user interfaces with the optimistic results from the comparative analysis of laptop and smartphone users' activity, suggest that the critical mass of users' activity required for users to fully understand the benefits of location-sharing can be achieved in a near future.

6 Conclusions

This project presents the findings of two studies, focusing on examining the dynamics of user privacy policy management in the context of location-sharing applications.

A first set of results was based on a study of a long-term usage population of a live location-sharing application, in which participants shared their location with real friends and acquaintances. A second set of results was reached based on a four-week field investigation of the same location-sharing application in similar conditions.

Our findings are the following:

- Social-based restrictions dominate the users' expressiveness spectrum. This type of restriction is also embedded of higher dynamics (compared to time-based and location-based restrictions), due to the inherent dynamics of social networks.
- When modifying their privacy policies through time, users typically evolve to less restrictive policies. Modifications that produce more restrictive privacy policies are exceptions.
- The privacy policies of users with higher number of iterations become more composite with each iteration, suggesting an increasing awareness of the implications of their decisions over time.
- In the process of defining their privacy policies, smartphone users require more iterations and a longer convergence period than laptop users. This suggests a higher level of privacy concern in respect to their locations and a more demanding attitude with the effectiveness of their privacy policies.
- Feedback mechanisms not only provide awareness but also influence the user's privacy policy management process with considerable probability. This is more noticeable for smartphone users.

7 References

[1] http://www.skyhookwireless.com/

[2] Landay, J. A., Joseph, A. D., and Reynolds, F. 2009. Guest Editors' Introduction: Smarter Phones. *IEEE Pervasive Computing* 8, 2, 12-13.

[3] Barkhuus, L. Dey, A. 2003. Location-based services for mobile telephony: a study of users' privacy concerns. In *9th International Conference of Human-Computer Interaction (INTERACT)*.

[4] Anthony, D., Henderson, T., and Kotz, D. 2007. Privacy in Location-Aware Computing Environments. *IEEE Pervasive Computing* 6, 4, 64-72.

[5] Tsai, J., Kelley, P., Cranor, L. Sadeh, N. 2009. Public perceptions of the risks and benefits of location-sharing technologies. In *37th Research Conference on Communication, Information, and Internet Policy (TPRC)*.

[6] Gruteser, M., Hoh, B., 2005. On the Anonimity of Periodic Location Samples. *2nd Int'l Conference Security in Pervasive Computing*, 179-192.

[7] Warren, S. D. and Brandeis, L. D. 1985. The right to privacy. In *Ethical Issues in the Use of Computers* Wadsworth Publ. Co., 172-183.

[8] Altman, I. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Brooks/Cole Pub. Co., Inc.

[9] Ferraiolo, D., Kuhn, R. 1992. Role-based access controls. In *Proceedings of 15th NIST-NCSC National Computer Security Conference*, 554-563

[10] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., Youman, C. E. 1996. Role-Based Access Control Models. *Computer*, 29, 2, 38-47.

[11] Saltzer, J. H., Schroeder, M. D. 1975. The Protection of Information in Computer Systems. *Proceedings of the IEEE* 63, 9.

[12] http://www.google.com/latitude/

[13] http://fireeagle.yahoo.net/

[14] http://xtify.com/

[15] http://www.loopt.com/

[16] http://foursquare.com/

[17] Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Comput.* 13, 6, 401-412.

[18] Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J., and Sadeh, N. 2009. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the 27th international Conference on Human Factors in Computing Systems*, 2003-2012.

[19] Ravichandran, R., Benisch, M., Kelley, P. G., and Sadeh, N. M. 2009. Capturing Social Networking Privacy Preferences. In *Proceedings of the 9th international Symposium on Privacy Enhancing Technologies*.

[20] Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. 2005. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 81-90.

[21] Lin, J., Hong, J., Sadeh, N. 2009. *Understanding People's Place Naming Preferences in Location Sharing*. Under review.

[22] Sun, J. Z., Sauvola, J. 2002. Mobility and mobility management: a conceptual framework. In *Proceedings of the 10th IEEE International Conference on Networks*, 205-210.

[23] Toninelli, A., Montanari, R., Lassila, O., and Khushraj, D. 2009. What's on Users' Minds? Toward a Usable Smart Phone Security Model. *IEEE Pervasive Computing* 8, 2, 32-39.

[24] E. Toch et al., 2009. *24/7: The Impact of Continuous Tracking on location sharing*. Under review.

[25] Smetters, D. K. and Good, N. 2009. How users use access control. In *Proceedings of the 5th Symposium on Usable Privacy and Security*,1-12.

[26] Kelley, P. G., Hankes Drielsma, P., Sadeh, N., and Cranor, L. F. 2008. User-controllable learning of security and privacy policies. In *Proceedings of the 1st ACM Workshop on Workshop on Aisec*, 11-18.

[27] Froehlich, J., Chen, M. Y., Consolvo, S., Harrison, B., and Landay, J. A. 2007. MyExperience: a system for *in situ* tracing and capturing of user feedback on mobile phones. In *Proceedings of the 5th international Conference on Mobile Systems, Applications and Services*, 57-70.

[28] Consolvo, S. and Walker, M. 2003. Using the Experience Sampling Method to Evaluate Ubicomp Applications. *IEEE Pervasive Computing* 2, 2, 24-31.

[29] Jensen, C., Potts, C., and Jensen, C. 2005. Privacy practices of Internet users: self-reports versus observed behavior. *Int. J. Hum.-Comput. Stud.* 63, 1-2, 203-227.

[30] http://locaccino.org/

[31] http://www.facebook.com/